Agence Nationale de Certification Electronique

TunTrust PKI

Certificate Policy / Certification Practice Statement

Version 06.1.4

	Wrote by	**Validated by**	**Approved by**
Function :	TunTrust	TunTrust Board of Directors	TunTrust Board of Directors
Date :	03/06/2026	15/07/2026	15/07/2026

Table of Contents

1 INTRODUCTION 10

1.1 OVERVIEW 10
1.2 DOCUMENT NAME AND IDENTIFICATION 10
1.3 PKI PARTICIPANTS 13
1.3.1 Certification Authorities (CA) 13
1.3.2 Registration Authorities 14
1.3.3 Subscribers 14
1.3.4 Relying parties 14
1.3.5 certificate managers 15
1.3.6 Other participants 15
1.4 CERTIFICATE USAGE 15
1.4.1 Appropriate Certificate uses 15
1.4.2 Prohibited Certificate Uses 15
1.5 POLICY ADMINISTRATION 15
1.5.1 Organization administering the document 15
1.5.2 Contact person 16
1.5.3 Person determining CP/CPS suitability for the policy 16
1.5.4 CP/CPS Approval Procedure 16
1.6 DEFINITIONS AND ACRONYMS 16
1.6.1 Definitions 16
1.6.2 Acronyms 25

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 25

2.1 REPOSITORIES 25
2.2 PUBLICATION OF CERTIFICATION INFORMATION 26
2.3 TIME OR FREQUENCY OF PUBLICATION 26
2.4 ACCESS CONTROLS ON REPOSITORIES 26

3 IDENTIFICATION AND AUTHENTICATION 27

3.1 NAMING 27
3.1.1 Types of names 27
3.1.2 Need for names to be meaningful 27
3.1.3 Anonymity or pseudonymity of Subscribers 27
3.1.4 Rules for interpreting various name forms 27
3.1.5 Uniqueness of names 27
3.1.6 Recognition, authentication, and role of trademarks 27
3.2 INITIAL IDENTITY VALIDATION 27
3.2.1 Method to prove possession of private key 28
3.2.2 Authentication of organization Identity 28
3.2.2.1 Identity 28
3.2.2.2 DBA/Tradename 28
3.2.2.3 Verification of country 29
3.2.2.4 Validation of Domain Authorization or Control 29
3.2.2.5 Authentication for an IP Address 32
3.2.2.6 Wildcard domain validation 32
3.2.2.7 Data Source Accuracy 33
3.2.2.8 CAA Records 33
3.2.2.8.1 DNSSEC Validation of CAA Records 33
3.2.2.9 Multi-Perspective Issuance Corroboration 33
3.2.3 Authentication of individual identity 36
3.2.4 Non-verified Subscriber information 37

3.2.5 Validation of Authority 37
3.2.6 Criteria for Interoperation 37
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 37
3.3.1 Identification and authentication for routine re-key 37
3.3.2 Identification and authentication for re-key after revocation 37
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 37

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 38

4.1 CERTIFICATE APPLICATION 38
4.1.1 Who can submit a Certificate application 38
4.1.2 Enrollment process and responsibilities 38
4.2 CERTIFICATE APPLICATION PROCESSING 39
4.2.1 Performing Identification and Authentication Functions 39
4.2.2 Approval Or Rejection Of Certificate Applications 40
4.2.2.1 CAA record processing 41
4.2.2.1.1 CAA Multi-Perspective Issuance Corroboration 42
4.2.2.1.2 CAA Parameters 42
4.2.2.1.3 DNSSEC Validation of CAA Records 42
4.2.3 Time to Process Certificate Applications 43
4.2.4 Certificate Authority Authorisation (CAA) 43
4.3 CERTIFICATE ISSUANCE 44
4.3.1 CA Actions during Certificate Issuance 44
4.3.1.1 Manual authorization of certificate issuance for Root CAs 44
4.3.1.2 Linting of to-be-signed Certificate content 44
4.3.1.3 Linting of issued Certificates 45
4.3.2 Notification to Subscriber by the CA of issuance of Certificate 45
4.4 CERTIFICATE ACCEPTANCE 45
4.4.1 Conduct Constituting Certificate Acceptance 45
4.4.2 Publication of the Certificate by the CA 45
4.4.3 Notification of Certificate issuance by the CA to other entities 45
4.5 KEY PAIR AND CERTIFICATE USAGE 46
4.5.1 Subscriber private key and Certificate usage 46
4.5.2 Relying Party Public Key and Certificate Usage 46
4.6 CERTIFICATE RENEWAL 46
4.6.1 Circumstances for Certificate Renewal 46
4.6.2 Who may request renewal 46
4.6.3 Processing Certificate renewal requests 46
4.6.4 Notification of new Certificate issuance to Subscriber 46
4.6.5 Conduct constituting acceptance of a renewal Certificate 47
4.6.6 Publication of the renewal Certificate by the CA 47
4.6.7 Notification of Certificate issuance by the CA to other entities 47
4.7 CERTIFICATE RE-KEY 47
4.7.1 Circumstance for Certificate re-key 47
4.7.2 Who may request certification of a new public key 47
4.7.3 Processing Certificate re-keying requests 47
4.7.4 Notification of new Certificate issuance to Subscriber 47
4.7.5 Conduct constituting acceptance of a re-keyed Certificate 47
4.7.6 Publication of the re-keyed Certificate by the CA 47
4.7.7 Notification of Certificate issuance by the CA to other entities 47
4.8 CERTIFICATE MODIFICATION 47
4.8.1 Circumstances for certificate modification 47
4.8.2 Who may request certificate modification 48
4.8.3 Processing certificate modification requests 48

4.8.4 Notification of new certificate issuance to subscriber 48
4.8.5 Conduct constituting acceptance of modified certificate 48
4.8.6 Publication of the modified certificate by the CA 48
4.8.7 Notification of certificate issuance by the CA to other entities 48
4.9 CERTIFICATE REVOCATION AND SUSPENSION 48
4.9.1 Circumstances For Revocation 48
4.9.1.1 Reasons for revoking a Subscriber Certificate 48
4.9.1.2 Reasons for revoking a Subordinate CA Certificate 49
4.9.2 Who can request revocation 50
4.9.3 Procedure for revocation request 50
4.9.4 revocation request grace period 51
4.9.5 Time within which CA must process the revocation request 51
4.9.6 Revocation checking requirement for relying parties 51
4.9.7 CRL Issuance Frequency 51
4.9.8 Maximum Latency for CRLs 52
4.9.9 On-line Revocation/Status Checking Availability 52
4.9.10 On-line revocation checking requirements 52
4.9.11 other forms of revocation advertisements available 52
4.9.12 Special requirements related to key compromise 52
4.9.13 Circumstances for suspension 53
4.9.14 who can request suspension 53
4.9.15 Procedure for suspension request 53
4.9.16 Limits on suspension Period 53
4.10 CERTIFICATE STATUS SERVICES 53
4.10.1 operational characteristics 53
4.10.2 Service Availability 53
4.10.3 Optional Features 53
4.11 END OF SUBSCRIPTION 54
4.12 KEY ESCROW AND RECOVERY 54
4.12.1 Key escrow and recovery Policy and practices 54
4.12.2 Session key encapsulation and recovery policy and practices 54

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 54

5.1 PHYSICAL CONTROLS 55
5.1.1 Site location and construction 55
5.1.2 Physical access 55
5.1.3 Power and air conditioning 56
5.1.4 Water Exposures 56
5.1.5 Fire Prevention and Protection 56
5.1.6 Media Storage 56
5.1.7 Waste Disposal 56
5.1.8 Off-Site Backup 56
5.2 PROCEDURAL CONTROLS 57
5.2.1 Trusted Roles 57
5.2.2 Number of persons required per task 58
5.2.3 Identification and authentication for each role 58
5.2.4 Roles requiring separation of duties 58
5.3 PERSONNEL CONTROLS 58
5.3.1 Qualifications, experience, and clearance requirements 58
5.3.2 Background check procedures 59
5.3.3 Training requirements 59
5.3.4 Retraining frequency and requirements 59

5.3.5 Job rotation frequency and sequence 59
5.3.6 Sanctions for unauthorized actions 60
5.3.7 Independent Contractor Requirements 60
5.3.8 Documentation Supplied to Personnel 60
5.4 AUDIT LOGGING PROCEDURES 60
5.4.1 Types of Events Recorded 60
5.4.1.1 Router and firewall activities logs 61
5.4.2 Frequency of processing log 61
5.4.3 Retention period for audit log 62
5.4.4 Protection of audit log 62
5.4.5 Audit log backup procedures 62
5.4.6 Audit collection System (Internal vs. External) 62
5.4.7 Notification to Event-Causing Subject 63
5.4.8 Vulnerability Assessments 63
5.5 RECORDS ARCHIVAL 63
5.5.1 Types of records archived 63
5.5.2 Retention period for archive 64
5.5.3 Protection of archive 64
5.5.4 Archive backup procedures 64
5.5.5 Requirements for time-stamping of records 64
5.5.6 Archive collection system (internal or external) 64
5.5.7 Procedures to obtain and verify archive information 64
5.6 KEY CHANGEOVER 65
5.7 COMPROMISE AND DISASTER RECOVERY 65
5.7.1 Incident and compromise handling procedures 65
5.7.1.1 Incident Response and Disaster Recovery Plans 65
5.7.1.2 Mass Revocation Plans 66
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 67
5.7.3 Entity Private Key Compromise Procedures 67
5.7.4 Business Continuity Capabilities After a Disaster 67
5.7.5 Miss-Issuance Handling procedures 68
5.8 CA OR RA TERMINATION 68

6 TECHNICAL SECURITY CONTROLS 69

6.1 KEY PAIR GENERATION AND INSTALLATION 69
6.1.1 KEY PAIR GENERATION 69
6.1.1.1 CA Key Pair Generation 69
6.1.1.2 RA Key Pair Generation 69
6.1.1.3 Subscriber Key Pair Generation 69
6.1.2 Private key delivery to Subscriber 70
6.1.3 Public key delivery to Certificate issuer 70
6.1.4 CA public key delivery to relying parties 70
6.1.5 Key sizes 70
6.1.5.1 Root CA Certificates 70
6.1.5.2 Subordinate CA Certificates 71
6.1.5.3 Subscriber Certificates 71
6.1.6 Public key parameters generation and quality checking 71
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 71
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 71
6.2.1 Cryptographic module standards and controls 72
6.2.2 Private key (n out of m) multi-person control 72
6.2.3 Private key escrow 72
6.2.4 Private key backup 72

6.2.5 Private key archival 73
6.2.6 Private key transfer into or from a cryptographic module 73
6.2.7 Private key storage on cryptographic module 73
6.2.8 Method of activating private key 73
6.2.9 Method of deactivating private key 73
6.2.10 Method of destroying private key 73
6.2.11 Cryptographic Module Rating 74
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 74
6.3.1 Public key archival 74
6.3.2 Certificate operational periods and key pair usage periods 74
6.4 ACTIVATION DATA 74
6.4.1 Activation data generation and installation 74
6.4.2 Activation data protection 75
6.4.3 Other aspects of activation data 75
6.5 COMPUTER SECURITY CONTROLS 75
6.5.1 Specific computer security technical requirements 75
6.5.2 Computer security rating 76
6.6 LIFE CYCLE TECHNICAL CONTROLS 76
6.6.1 System development controls 76
6.6.2 Security management controls 76
6.6.3 Life cycle security controls 76
6.7 NETWORK SECURITY CONTROLS 77
6.7.1 Network Segmentation 78
6.7.2 CA Infrastructure Security 78
6.8 TIME-STAMPING 79

7 CERTIFICATE, CRL, AND OCSP PROFILES 79

7.1 CERTIFICATE PROFILE 79
7.1.1 Version number(s) 79
7.1.2 Certificate extensions 79
7.1.2.1 Root CA Certificate Profile 79
7.1.2.1.1 Root CA Validity 80
7.1.2.1.2 Root CA Extensions 80
7.1.2.1.3 Root CA Authority Key Identifier 80
7.1.2.1.4 Root CA Basic Constraints 81
7.1.2.2 Cross-Certified Subordinate CA Certificate Profile 81
7.1.2.3 Technically Constrained Non-TLS Subordinate CA Certificate Profile 81
7.1.2.4 Technically Constrained Precertificate Signing CA Certificate Profile 81
7.1.2.5 Technically Constrained TLS Subordinate CA Certificate Profile 81
7.1.2.5.1 Technically Constrained TLS Subordinate CA Extensions 81
7.1.2.5.2 Technically Constrained TLS Subordinate CA Name Constraints 82
7.1.2.6 TLS Subordinate CA Certificate Profile 84
7.1.2.6.1 TLS Subordinate CA Extensions 84
7.1.2.7 Subscriber (Server) Certificate Profile 85
7.1.2.7.1 Subscriber Certificate Types 86
7.1.2.7.2 Domain Validated 86
7.1.2.7.3 Individual Validated 86
7.1.2.7.4 Organization Validated 86
7.1.2.7.5 Extended Validation 88
7.1.2.7.6 Subscriber Certificate Extensions 88
7.1.2.7.7 Subscriber Certificate Authority Information Access 88
7.1.2.7.8 Subscriber Certificate Basic Constraints 89
7.1.2.7.9 Subscriber Certificate Certificate Policies 89
7.1.2.7.10 Subscriber Certificate Extended Key Usage 90

7.1.2.7.11 Subscriber Certificate Key Usage 90
7.1.2.7.12 Subscriber Certificate Subject Alternative Name 91
7.1.2.8 OCSP Responder Certificate Profile 92
7.1.2.8.1 OCSP Responder Validity 93
7.1.2.8.2 OCSP Responder Validity 93
7.1.2.8.3 OCSP Responder Authority Information Access 93
7.1.2.8.4 OCSP Responder Basic Constraints 94
7.1.2.8.5 OCSP Responder Extended Key Usage 94
7.1.2.8.6 OCSP Responder id-pkix-ocsp-nocheck 94
7.1.2.8.7 OCSP Responder Key Usage 94
7.1.2.8.8 OCSP Responder Certificate Policies 95
7.1.2.9 Precertificate Profile 95
7.1.2.9.1 Precertificate Profile Extensions - Directly Issued 96
7.1.2.9.2 Precertificate Profile Extensions - Precertificate CA Issued 97
7.1.2.9.3 Precertificate Poison 97
7.1.2.9.4 Precertificate Authority Key Identifier 97
7.1.2.10 Common CA Fields 97
7.1.2.10.1 CA Certificate Validity 97
7.1.2.10.2 CA Certificate Naming 97
7.1.2.10.3 CA Certificate Authority Information Access 99
7.1.2.10.4 CA Certificate Basic Constraints 99
7.1.2.10.5 CA Certificate Certificate Policies 99
7.1.2.10.6 CA Certificate Extended Key Usage 101
7.1.2.10.7 CA Certificate Key Usage 101
7.1.2.10.8 CA Certificate Name Constraints 101
7.1.2.11 Common Certificate Fields 103
7.1.2.11.1 Authority Key Identifier 103
7.1.2.11.2 CRL Distribution Points 103
7.1.2.11.3 Signed Certificate Timestamp List 104
7.1.2.11.4 Subject Key Identifier 104
7.1.2.11.5 Other Extensions 104
7.1.3 Algorithm object identifiers 104
7.1.3.1 SubjectPublicKeyInfo 105
7.1.3.2 Signature AlgorithmIdentifier 105
7.1.4 Name forms 105
7.1.4.1 Name Encoding 105
7.1.4.2 Subject Attribute Encoding 106
7.1.4.3 Subscriber Certificate Common Name Attribute 108
7.1.4.4 Other Subject Attributes 108
7.1.5 Name constraints 109
7.1.6 Certificate policy object identifier 109
7.1.6.1 RESERVED CERTIFICATE POLICY IDENTIFIERS 109
7.1.6.2 Root CA Certificates 109
7.1.6.3 Subordinate CA Certificates 109
7.1.6.4 Subscriber Certificates 109
7.1.7 Usage of Policy Constraints extension 109
7.1.8 Policy Qualifiers Syntax and Semantics 110
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 110
7.2 CRL PROFILE 110
7.2.1 Version Number(s) 111
7.2.2 CRL and CRL Entry Extensions 111
7.2.2.1 CRL Issuing Distribution Point 113
7.3 OCSP PROFILE 113
7.3.1 Version Number 114
7.3.2 OCSP Extensions 114

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 114

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT 114
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR 114
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 115
8.4 TOPICS COVERED BY ASSESSMENT 115
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 115
8.6 COMMUNICATION OF RESULTS 115
8.7 SELF-AUDITS 116

9 OTHER BUSINESS AND LEGAL MATTERS 116

9.1 FEES 116
9.1.1 Certificate issuance or renewal fees 116
9.1.2 Certificate access fees 116
9.1.3 Revocation or status information access fees 117
9.1.4 Fees for other services 117
9.1.5 Refund Policy 117
9.2 FINANCIAL RESPONSIBILITY 117
9.2.1 Insurance coverage 117
9.2.2 Other assets 117
9.2.3 Insurance or warranty coverage for end-entities 117
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 117
9.3.1 Scope of confidential information 117
9.3.2 Information not within the scope of confidential information 118
9.3.3 Responsibility to protect Confidential Information 118
9.4 PRIVACY OF PERSONAL INFORMATION 118
9.4.1 Privacy Plan 118
9.4.2 Information treated as private 118
9.4.3 Information not deemed private 118
9.4.4 Responsibility to protect private information 118
9.4.5 Notice and consent to use private information 118
9.4.6 Disclosure pursuant to judicial or administrative process 119
9.4.7 Other information disclosure circumstances 119
9.5 INTELLECTUAL PROPERTY RIGHTS 119
9.6 REPRESENTATIONS AND WARRANTIES 119
9.6.1 CA representations and warranties 119
9.6.2 RA representations and warranties 120
9.6.3 Subscriber representations and warranties 120
9.6.4 Relying party representations and warranties 121
9.6.5 Representations and warranties of other participants 121
9.7 DISCLAIMERS OF WARRANTIES 122
9.8 LIMITATIONS OF LIABILITY 122
9.9 INDEMNITIES 122
9.9.1 Indemnification by TunTrust 122
9.9.2 Indemnification by Subscribers 123
9.9.3 Indemnification by Relying Parties 123
9.10 TERM AND TERMINATION 123
9.10.1 Term 123
9.10.2 Termination 123
9.10.3 Effect of termination and survival 123
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 123
9.12 AMENDMENTS 124

9.12.1 Procedure for amendment 124
9.12.2 Notification mechanism and period 124
9.12.3 Circumstances under which OID must be changed 124
9.13 DISPUTE RESOLUTION PROVISIONS 124
9.14 GOVERNING LAW 124
9.15 COMPLIANCE WITH APPLICABLE LAW 124
9.16 MISCELLANEOUS PROVISIONS 124
9.16.1 Entire agreement 124
9.16.2 Assignment 125
9.16.3 Severability 125
9.16.4 Enforcement (attorneys' fees and waiver of rights) 125
9.16.5 Force Majeure 125
9.17 OTHER PROVISIONS 125
APPENDIX A: TUNTRUST CA CERTIFICATE PROFILES 126
APPENDIX B : TUNTRUST PKI END-ENTITY PROFILES 129
APPENDIX C : PROFILES OF THE CRL OF TUNTRUST CAS 133
APPENDIX D : OCSP PROFILE DESCRIPTION 135

1 INTRODUCTION

1.1 OVERVIEW

The Agence Nationale de Certification Electronique was founded in accordance with Law no. 2000-83 of 9 August 2000 governing electronic exchanges and commerce in Tunisia. The Agence Nationale de Certification Electronique is a government-owned Certificate Authority (CA) and will be referred to in the remainder of this document with its trademark name “TunTrust”.

In this document, the words “TunTrust” and “TunTrust CA” and “TunTrust PKI” are used interchangeably and include the TunTrust Root CAs and Issuing CAs of the Agence Nationale de Certification Electronique.

Referred as Certificate Policy and Certification Practice Statement (CP/CPS), this document has been prepared in compliance with the guide book of “IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” for the purpose of describing how TunTrust executes its operations during providing OV SSL (Organization Validated SSL) certificates to domain names restricted by the “.tn” top-level domain for Tunisia and owned by entities operating under the Tunisian Jurisdiction.

TunTrust conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

TunTrust also adheres to the latest published versions of the Chrome Root Program Policy and the Common CA Database (CCADB) Policy. In case of any inconsistency between this document and those policies, the external policies shall supersede.

This CP/CPS document describes the execution of the services in regard to accepting Certificate applications, Certificate issuance and management, and Certificate revocation procedures in compliance with administrative, technical and legal requirements.

This CP/CPS also determines practice responsibilities and obligations of TunTrust, applicants, subscribers and relying parties that use or rely on Certificates issued by TunTrust.

Pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this CP/CPS is divided into nine parts that cover the security controls and practices and procedures for Certificate services operated by TunTrust. To preserve the outline specified by RFC 3647, section headings that do not apply are accompanied with the statement “Not applicable” or “No stipulation” along with a brief explanation of the reason.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is the CP/CPS followed by TunTrust while providing OV SSL certification services and was approved for publication by the TunTrust Board of Directors. This CP/CPS document is disclosed to the public at https://www.tuntrust.tn/repository.

Note: The OID of TunTrust is joint-iso-itu-t(2) country(16) tn(788) public-sector(1) public-sector-enterprises(2) tuntrust(7). The OID of the present document is: 2.16.788.1.2.7.1.1

Revisions of this document have been made as follows:

Version	Date	Comment	Changes
00	19 November 2018	Draft	The whole document
01	12 April 2019	The first CP/CPS document for public	The whole document
02	30 April 2019	The second version of the CP/CPS	Appendix A, B and C
03	20 September 2019	The third version of the CP/CPS	Sections 1.3, 1.4.2, 1.5, 1.6, 2.2, 2.3, 2.4, 3.1, 3.2, 4.1, 4.2.1, 4.3.1, 4.4.1, 4.9, 4.10.2, 4.12.2, 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 6.1, 6.2, 6.3, 6.4, 6.5, 6.5.2, 6.6, 6.7, 7.1, 7.2.1, 7.3.2, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 9, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.9, 9.11, 9.12, 9.14, 9.15 and 9.16
04	02 October 2019	The fourth version of the CP/CPS	Sections 1.3.1, 4.2.1, 4.9.3, 4.10.2, 5.4.4, 5.5.1, 5.5.2, 5.5.3, 6.7.2, 7.1.2, 7.1.4 and 7.2.2
04.1	26 May 2020	Complying with the CA/B Forum SC23, SC24, SC25 & SC27 ballots	Sections 1.6.1, 3.2.2.4, 3.2.2.4.4, 3.2.2.4.18, 3.2.2.4.19, 3.2.2.6, 3.2.2.8, 4.2.2, 4.9.10 and 6.1.5.
04.2	24 August 2020	Complying with the CA/B Forum SC31 and SC33 ballots	Sections 1.6.1, 3.2.2.4.13, 3.2.2.4.20, 3.2.2.8, 4.9.1, 4.9.10, 6.1.1, 6.1.1.3, 6.1.5, 6.3.2, 7.1.2.4, 7.1.3.1, 7.1.3.2, 7.1.4.1, 7.1.6.4, 7.2.2, 7.3, 7.3.2, 8.6, 9.6.3 and Appendix C
04.3	27 August 2020	Clean-up and fixing typos	Sections 11.6.1, 4.2.1, 4.3.1, 4.9.1.1, 7.1.2.4, 7.1.3.1, 7.1.3.2 and Appendix B.1.
04.4	01 December 2020	Complying with the CA/B Forum Ballots SC28 & SC35 and Comments on the Bug 1587779	Sections 1.5.2, 1.6.1, 2.2, 3.2.2.8, 4.2.4, 4.3.1, 4.9.1, 4.9.3, 5.4.1, 5.4.3, 5.7.3, 6.1.1, 6.1.1.2, 7.1.2.4, 7.1.4.2.1 and Appendix B
04.5	02 December 2020	Add more details about Certificate Problem Reporting	Section 1.5.2
04.6	14 April 2021	Exceptions for CAA records checking	Section 4.2.4
04.7	30 April 2021	Methods to demonstrate private key compromise Omitting examples of the public suffix & registry-controlled labels	Sections 4.9.12 and 3.2.2.6
04.8	20 September 2021	Complying with the CA/B Forum Ballot SC46 & 48	Sections 1.6.1, 1.6.2, 3.1.2, 3.2.2.4, 3.2.2.4.2, 3.2.2.4.4, 3.2.2.4.13, 3.2.2.4.14, 3.2.2.6, 4.2.2,

			7.1.4.2.1 & Appendix B
04.9	08 April 2022	Complying with the CA/B Forum Ballot SC50, SC51 & SC53	Sections 1.6.1, 5.4.1, 5.4.2, 5.4.3, 5.4.4, 5.4.5, 5.4.6, 5.5.1, 5.5.2 and 7.1.3.2
05	16 January 2023	Complying with the CA/B Forum SC56 ballot	Sections 1.2, 1.6.1, 3.2.2.2, 6.3.2, 8, 9.6.1 and 9.15
05.1	12 September 2023	Revocation of TunTrust Qualified CA, Complying with the CA/B Forum SC61, SC62 and SC63 ballots	Sections 1.3.1, 1.6.1, 3.2.6, 4.2.2, 4.9.1.1, 4.9.7, 4.9.9, 4.9.10, 6.1.7, 7.1, 7.1.2 (& subsections), 7.1.4 (& subsections), 7.1.5, 7.1.6.1, 7.1.6.3, 7.1.6.4, 7.2, 7.2.2, 7.2.2.1, 8.1,8.5, 8.6, 9.6.1, A.2, C.2 and D
05.2	01 March 2024	Complying with the CA/B Forum SC-066 and Section 6 of RFC 3647, correcting typos related to SC62 and adding hypertext links to sections.	Sections 1.1, 1.6.1, 1.6.2, 2.2, 6.2, 7.1, 7.1.2.11.4, 7.1.6.4, 8, Section Headings of 1.3.1, 1.4.1, 3.2.2.4.10, 4.7.1, 4.7.3, 4.9.1, 4.9.6, 5.4.2, 5.7.2, 7, 7.1.2
05.3	24 May 2024	Complying with the CA/B Forum SC69	Section 5.4.1 & 5.4.1.1
05.4	02 September 2024	Complying with the CA/B Forum SC65, SC73 and SC75	Sections 1.3.3, 1.6.1, 4.3.1.1, 4.3.1.2, 4.3.1.3, 4.9.1.1, 6.1.1.3, 6.3.2, 6.6.1 and 8.7
05.5	30 October 2024	Complying with the CA/B Forum ballot SC76 and introducing the use of governmental webservices for identity validation	Sections 3.2.2.1, 3.2.2.4.7, 4.2.1, 4.9.9 & 4.9.10
05.6	16 December 2024	Correcting typos and complying with the CA/B Forum ballot SC78	Section 4.10.3, 7.1.2.7.4 & Appendix B
05.7	03 February 2025	Adding Method 3.2.2.4.19	Section 3.2.2.4.19
05.8	15 March 2025	Complying with the CA/B Forum ballot SC083, SC067 & SC084, updating domain validation methods, and correcting internal links.	Sections 1.5.2, 1.6.1, 2.2, 2.3, 3.2.2.1, 3.2.2.2, 3.2.2.9, 3.2.2.4.7, 3.2.2.4.13, 3.2.2.4.14, 3.2.2.4.19, 3.2.2.4.21, 4.12.1, 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.3.2, 5.3.4, 6.1.1.1, 6.2.2, 6.4.1, 6.4.3, 6.7, 7.1, 7.1.2.1.2, 7.1.2.7.4, 7.1.2.7.12, 7.1.2.105, 7.1.2.10.6 & APPENDIX B
05.9	24 March 2025	Updating OVCP SSL certificate profile	APPENDIX B
06	11 June 2025	Change in Profile & Complying with the CA/B Forum ballot SC81	Sections 1.6.1, 4.2.1, 5.7.2, 6.3.2 & Appendix B

06.1	08 September 2025	Correcting typos, and complying with the CA/B Forum ballot NS-007	Section 3.2.2.4.2 & 6.7
06.1.1	01 December 2025	Comply with Google Chrome Policy, Ballot SC088, SC089, correcting typos, add certificate profile of 30 days	Section 3.2.2.4.22, 4.1.2, 4.2.1, 5.7.1.1, 5.7.1.2, Appendix B
06.1.2	15 January 2026	Correcting typos	Appendix B, Section 3.2.2.9
06.1.3	12 March 2026	Complying with ballots SC94 and SC-96	Section 3.2.2.4, 3.2.2.8.1 and Appendix B
06.1.4	15/07/2026	Correcting missing parts from ballot NS-008, correcting typos, following the cleanup ballot SC-095v3 and complying with ballots SC-99 and SC098	1.6.1, 3.1.5, 3.2.2.4, 3.2.2.4.4, 3.2.2.4.19, 3.2.2.8, 3.2.2.8.1, 3.2.2.9, 4.2.1, 4.2.2, 4.2.2.1, 4.2.2.1.1, 4.2.2.1.2, 4.2.2.1.3, 4.3.1.2, 4.9.1.1, 5.4.1, 5.4.8, 5.5.1, 5.5.2, 5.7.1.2, 5.7.2, 6.3.2,6.7.1, 6.7.2, 7.1, 7.1.2.7.1, 7.1.2.7.7, 7.1.2.8, 7.1.2.8.2, 7.1.2.8.3, 7.1.2.8.3, 7.1.2.8.8, 7.1.2.9, 7.1.2.10.3, 7.2

1.3 PKI PARTICIPANTS

PKI Participants defined within the scope of this document are the parties bearing relevant rights and obligations within OV SSL certification services of TunTrust.

These parties are defined as CA, Registration Authority, Subscribers, Certificate Managers and Relying Parties.

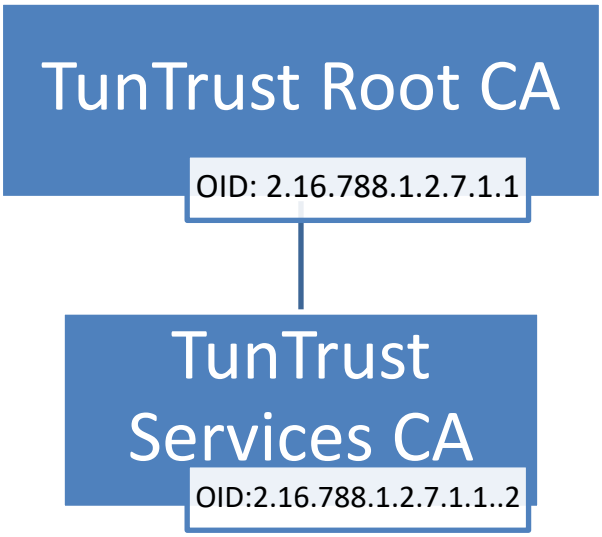
1.3.1 CERTIFICATION AUTHORITIES (CA)

TunTrust CA provides OV SSL certification services in accordance with this CP/CPS. As a CA, TunTrust performs functions associated with Public Key operations, including receiving Certificate requests, issuing, and revoking OV SSL Certificates, and maintaining, issuing, and publishing CRLs and OCSP responses.

The TunTrust PKI consists of a two-level CA hierarchy:

- **TunTrust Root CA**: root-signing all TunTrust issuing CAs and kept offline.
- **TunTrust Services CA**: This issuing CA is restricted to only issue OV SSL certificates to domain names under ".tn" top-level domain and owned by entities operating under the Tunisian Jurisdiction.

Certificate profiles of TunTrust PKI are detailed in Appendix A.



1.3.2 REGISTRATION AUTHORITIES

TunTrust does not delegate the execution of Section 3.2 requirement to a Delegated Third Party. TunTrust operates an internal Registration Authority located in the same infrastructure as its CA offerings, referred to in this document as TunTrust RA, where all registration procedures are directly executed by TunTrust personnel as described in Section 3.2.

TunTrust personnel involved in the issuance of OV SSL certificates must meet and follow the requirements set out in Sections 4.2 and 5.3.

TunTrust RA manages and performs the following roles and responsibilities:

- Identifying and authenticating Applicants for Certificates,
- Accepting, evaluating, approving or rejecting the registration of Certificate applications,
- Using authorized documents or sources of information to evaluate and authenticate an Applicant's application,
- Initiating the process to revoke a Certificate from the TunTrust CA,
- Archiving of the registration files (electronic and / or paper).

1.3.3 SUBSCRIBERS

Subscribers are legal entities under the Tunisian Jurisdiction who apply for OV SSL Certificates from TunTrust CA and agree to be bound by the relevant Subscriber Agreement. In this document, a Subscriber who has registered, but not yet received, a Certificate is referred to as an Applicant.

In some situations, TunTrust acts as an Applicant or Subscriber, for instance, when it generates and protects a Private Key, requests a Certificate, demonstrates control of a Domain, or obtains a Certificate for its own use.

1.3.4 RELYING PARTIES

A Relying party is any natural person or legal entity that relies on a Valid OV SSL Certificate issued by TunTrust CA. Relying Parties are responsible for verifying the validity of the Certificates.

To verify the validity of a Certificate, Relying Parties can refer to the CRL or OCSP response. The locations of the CRL distribution point and OCSP responder are detailed within the Certificate.

1.3.5 CERTIFICATE MANAGERS

As part of this CP/CPS, a Certificate Manager is a natural person who is either Applicant, employed by Applicant, or an authorized agent who has express authority to represent Applicant and is responsible for the use of the certificate (and associated private key).

Certificate Managers must meet the conditions and obligations that are set in this CP/CPS and in the Subscriber Agreement. The Certificate is attached to the Subscriber and not to the Certificate Manager. In case of change of Certificate Manager, the Subscriber shall report it to TunTrust and appoint a successor.

1.3.6 OTHER PARTICIPANTS

In the addition to the PKI participants described in Sections 1.3.2, 1.3.3 and 1.3.4, TunTrust will involve other parties as needed. TunTrust will contractually obligate each party to comply with all applicable requirements in this CP/CPS and monitor its compliance.

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

OV SSL Certificates are used to secure online communication and transactions where the risks of data compromise and fraud exist. The OV SSL Certificate allows the end entity to prove its identity to other participants and maintaining the integrity of the transaction.

At all times, Subscribers are required to use Certificates in accordance with this CP/CPS and all applicable laws and regulations.

1.4.2 PROHIBITED CERTIFICATE USES

Certificate use is restricted by using Certificate extensions on key usage and extended key usage. Any usage of the Certificate inconsistent with these extensions is not authorized.

Certificates issued under this CP/CPS may not be used (i) for any application requiring fail safe performance such as (a) air traffic control systems, (b) aircraft navigation systems, (c) weapons control systems, or (e) any other system whose failure could lead to injury, death or environmental damage; or (ii) where prohibited by law.

OV SSL Certificates issued under this CP/CPS do not guarantee that the Subject is trustworthy, operating a reputable business or that the equipment on which the Certificate has been installed is not free from defect, malware or virus.

1.5 POLICY ADMINISTRATION

1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT

The organization administering the CP/CPS is TunTrust. Its Board of Directors acts as the Certificate Policy Authority. The Board of Directors is composed of the senior management of TunTrust. The TunTrust Board of Directors is the highest level management body with final authority and responsibility for:

- Specifying and approving the TunTrust infrastructure and practices,
- Approving the TunTrust CP/CPS,
- Defining the review process for practices and policies including responsibilities for maintaining the CP/CPS,
- Defining the review process that ensures that TunTrust CAs properly implement the above practices,
- Publication to the Subscribers and Relying Parties of the CP/CPS and its revisions.

1.5.2 CONTACT PERSON

TunTrust Certificate Policy Authority may be contacted at the following address:

TUNTRUST - Agence Nationale de Certification Electronique

Policy Authority

Technopark El Ghazala, Road of Raoued, Ariana 2083, Tunisia

Tel.: +216 70 834 600

Mail : pki@tuntrust.tn

Web : https://www.tuntrust.tn

Subscribers, Relying Parties, Application Software Suppliers, and other third parties can submit Certificate Problem reports of suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates via email to revoke@tuntrust.tn. Further details are available in https://www.tuntrust.tn/content/revocation-certificat.

1.5.3 PERSON DETERMINING CP/CPS SUITABILITY FOR THE POLICY

The Certificate Policy Authority is responsible for determining the suitability and applicability of this CP/CPS based on the results and recommendations received from a Qualified Auditor as specified in Section 8.

1.5.4 CP/CPS APPROVAL PROCEDURE

TunTrust Certificate Policy Authority will approve the CP/CPS, along with any amendments. Any amendments made to the CP/CPS will be reviewed by the Certificate Policy Authority for consistency with the practices that are implemented prior to its approval. Changes made will be tracked within the revision table. Refer to Section 9.12 below for CP/CPS amendment procedure.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 DEFINITIONS

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate is issued, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate request.

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a Certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.

Application Software Supplier: A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

Attestation Letter: A letter attesting that Subject Information is correct written by an accountant, lawyer, government official or other reliable third party customarily relied upon for such information.

Audit Period: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in section 8.18.1.

Audit Report: A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of the CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates.

Authorization Domain Name: The FQDN used to obtain authorization for Certificate issuance for a given FQDN to be included in a Certificate. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If a Wildcard Domain Name is to be included in a Certificate, then the CA MUST remove "*." from the left-most portion of the Wildcard Domain Name to yield the corresponding FQDN. The CA may prune zero or more Domain Labels of the FQDN from left to right until encountering a Base Domain Name and may use any one of the values that were yielded by pruning (including the Base Domain Name itself) for the purpose of domain validation.

Authorized Ports: One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh).

Base Domain Name: The portion of an applied-for FQDN that is the first Domain Name node left of a registry controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most Domain Name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

Baseline Requirements: The Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates as published by the CA/Browser Forum and any amendments to such document.

CAA: From RFC 8659 (https://tools.ietf.org/html/rfc8659): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue Certificates for that domain name. CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended Certificate mis-issue."

CA Key Pair: A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).

CA Infrastructure: Collectively the infrastructure used by the CA or Delegated Third Party which qualifies as a:
• Certificate System;

• Root CA System (Air-Gapped and otherwise); or

• Security Support System.

Certificate: An electronic document that uses a digital signature to bind a public key and an identity.

Certificate Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Profile: A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 of the Baseline Requirements. e.g. a Section in a CA's CPS or a certificate template file used by CA software.

Certificate System: The system used by a CA or Delegated Third Party in providing identity verification, registration and enrollment, certificate approval, issuance, validity status, support, storage and other PKI-related services.

Certificate Transparency: To ensure Certificates function properly throughout their lifecycle, TunTrust will log SSL Certificates with a public Certificate transparency database if the subscriber signs the subscriber agreement and therefore opts for the publication of the log containing information relating to his certificate. Because this will become a requirement for Certificate functionality, Subscriber cannot opt out of this process. Log server information is publicly accessible. Once submitted, information cannot be removed from a log server.

Certificate Revocation List: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Root CAs and Subordinate CAs.

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Control: "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors ; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

Country: Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

Cross -Certified Subordinate CA Certificate: A Certificate that is used to establish a trust relationship between two CAs.

Critical Security Event: An event, set of circumstances, or anomalous activity that could lead to:

1. a circumvention of CA Infrastructure security controls; or

2. A compromise of TunTrust's Infrastructure integrity or operational continuity

These include, but are not limited to:

1. excessive login attempts;

2. attempts to access prohibited resources;

3. denial of service and distributed denial of service attacks;

4. attacker reconnaissance;

5. excessive traffic at unusual hours;

6. signs of unauthorized access;

7. system intrusion; or

8. physical compromise of component integrity

CSPRNG: A random number generator intended for use in a cryptographic system.

Delegated Third Party: A natural person or Legal Entity that is not the CA, and whose activities are not within the scope of the appropriate CA audits, but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

DNS CAA Email Contact: The email address defined in section A.1.1 of the Baseline Requirements.

DNS CAA Phone Contact: The phone number defined in Section A.1.2 of the Baseline Requirements.

DNS TXT Record Email Contact: The email address defined in Section A.2.1of the Baseline Requirements.

DNS TXT Record Phone Contact: The phone number defined in Section A.2.2of the Baseline Requirements.

Domain Contact: The Domain Name Registrant, technical contact, or administrative contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.

Domain Label: From RFC 8499 (<https://tools.ietf.org/html/rfc8499>): "An ordered list of zero or more octets that makes up a portion of a domain name. Using graph theory, a label identifies one node in a portion of the graph of all possible domain names."

Domain Name: An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.

Domain Namespace: The set of all possible Domain Names those are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain

Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assignees).

Expiry Date: The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

Fully-Qualified Domain Name: A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name System.

Government Agency: In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of Private Organizations is established (e.g., the government agency that issued the Certificate of Incorporation). In the context of Business Entities, the government agency in the jurisdiction of operation that registers business entities. In the case of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

High Risk Certificate Request: A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected Certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.

Individual: A natural person.

Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of Certificate issuance because it does not end with a Top-Level Domain registered in IANA's Root Zone Database.

IP Address: A 32-bit or 128-bit number assigned to a device that uses the Internet Protocol for communication.

IP Address Contact: The person(s) or entity(ies) registered with an IP Address Registration Authority as having the right to control how one or more IP Addresses are used.

IP Address Registration Authority: The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person or an unauthorized person has had access to it

Key Generation Script: A documented plan of procedures for the generation of a CA Key Pair.

Key Pair: The Private Key and its associated Public Key.

LDH Label: From RFC 5890 (<https://tools.ietf.org/html/rfc5890>): "A string consisting of ASCII letters, digits, and the hyphen with the further restriction that the hyphen cannot appear at the beginning or end of the string. Like all DNS labels, its total length must not exceed 63 octets."

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Linting: A process in which the content of digitally signed data such as a Precertificate [RFC 6962], Certificate, Certificate Revocation List, or OCSP response, or data-to-be-signed object such as a `tbsCertificate` (as described in [RFC 5280, Section 4.1.1.1]) is checked for conformance with the profiles and requirements defined in the Baseline Requirements.

Multi-Factor Authentication: An authentication mechanism consisting of two or more of the following independent categories of credentials (i.e. factors) to verify the user's identity for a login or other transaction: something you know (knowledge factor), something you have (possession factor), and something you are (inherence factor). Each factor must be independent. Certificate based authentication can be used as part of Multifactor Authentication only if the private key is stored in a Secure Key Storage Device.

Multi-Perspective Issuance Corroboration: A process by which the determinations made during domain validation and CAA checking by the Primary Network Perspective are corroborated by other Network Perspectives before Certificate issuance.

Network Perspective: Related to Multi-Perspective Issuance Corroboration. A system (e.g., a cloud-hosted server instance) or collection of network components (e.g., a VPN and corresponding infrastructure) for sending outbound Internet traffic associated with a domain control validation method and/or CAA check. The location of a Network Perspective is determined by the point where unencapsulated outbound Internet traffic is typically first handed off to the network infrastructure providing Internet connectivity to that perspective.

Network Boundary Control: Components that manage and control network traffic flow to, from, and within Tuntrust's Infrastructure.

Non-Reserved LDH Label: From RFC 5890 (https://tools.ietf.org/html/rfc5890): "The set of valid LDH labels that do not have ' `--` ' in the third and fourth positions."

Object Identifier: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol: An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

Parent Company: A company that Controls a Subsidiary Company.

Pending Prohibition: The use of a behavior described with this label is highly discouraged, as it is planned to be deprecated and will likely be designated as MUST NOT in the future.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Principle of Least Privilege: The principle that users, devices, and software should only have the minimum necessary access and privileges to complete their functions.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure: A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Physically Secure Environment: A controlled and protected physical space consisting minimally of a physical environment which is:

1. protected by security controls which address the topics outlined in section 4.5.1 of RFC 3647;
2. and 2. Operated in accordance with Risk Assessments conducted by the CA.

P-Label: A XN-Label that contains valid output of the Punycode algorithm (as defined in RFC 3492, Section 6.3) from the fifth and subsequent positions.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.2 of the CA/B Forum Baseline Requirements.

Random Value: A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the Certificate application process or revocation process or both. When “RA” is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate. Relying Parties must read and agree to TunTrust’s relying party agreement available at https://www.tuntrust.tn/repository.

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Request Token: A value derived in a method specified by the CA which binds this demonstration of control to the certificate request. The Request Token SHALL incorporate the key used in the certificate request. A Request Token MAY include a timestamp to indicate when it was created. A Request Token MAY include

other information to ensure its uniqueness. A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation. A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future. A Request Token that does not include a timestamp is valid for a single use and the CA SHALL NOT re-use it for a subsequent validation. The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.

Note: Examples of Request Tokens include, but are not limited to:

(i) a hash of the public key; or

(ii) a hash of the Subject Public Key Info [X.509]; or

(iii) a hash of a PKCS#10 CSR.

A Request Token may also be concatenated with a timestamp or other data. If a CA wanted to always use a hash of a PKCS#10 CSR as a Request Token and did not want to incorporate a timestamp and did want to allow certificate key re-use then the applicant might use the challenge password in the creation of a CSR with OpenSSL to ensure uniqueness even if the subject and key are identical between subsequent requests.

Note: This simplistic shell command produces a Request Token which has a timestamp and a hash of a CSR.

echo `date -u +%Y%m%d%H%M` `sha256sum <r2.csr` \| sed "s/[-]//g"

The script outputs:

201602251811c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f

Required Website Content: Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.

Requirements: The Baseline Requirements of the CA/B Forum.

Reserved IP Address: An IPv4 or IPv6 address that is contained in the address block of any entry in either of the following IANA registries:
https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml

https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

Root CA: The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root CA System: A system used to create a Root Certificate or to generate, store, or sign with the Private Key associated with a Root Certificate.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Root Key Generation Script: A documented plan of procedures to be performed for the generation of the Root CA Key Pair.

Secure Key Storage Device: A device certified as meeting at least FIPS 140-2 level 2 overall, level 3 physical, or Common Criteria (EAL 4+).

Security Support System: The System supporting the security of the CA Infrastructure, performing functions such as: 1. authentication; 2. audit logging; 3. audit log reduction and analysis; 4. vulnerability scanning; 5. physical intrusion detection; 6. host-based intrusion detection; and 7. network-based intrusion detection.

Short-lived Subscriber Certificate: For Certificates issued on or after 15 March 2024 and prior to 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 10 days (864,000 seconds). For Certificates issued on or after 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 7 days (604,800 seconds).

Sovereign State: A state or country that administers its own government, and is not dependent upon, or subject to, another power.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name or an IP Address listed in the subjectAltName extension or the Subject commonName field.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement.

Subscriber Agreement: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties available at https://www.tuntrust.tn/repository.

Subsidiary Company: A company that is controlled by a Parent Company.

Technically Constrained Subordinate CA Certificate: A Subordinate CA Certificate which uses a combination of Extended Key Usage and/or Name Constraint extensions, as defined within the relevant Certificate Profiles of the Baseline Requirements to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.

Test Certificate: This is no longer used in the Baseline Requirements.

Trustworthy System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

Trusted Role: An individual employee or contractor of a CA or Delegated Third Party who has authorized access to any Certificate System or Root CA System

Unregistered Domain Name: A Domain Name that is not a Registered Domain Name.

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialist: Someone who performs the information verification duties specified by these Requirements.

Validity Period: From RFC 5280 (https://tools.ietf.org/html/rfc5280) : "The period of time from notBefore through notAfter, inclusive".

WHOIS: Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.

Wildcard Certificate: A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names contained in the Certificate.

Wildcard Domain Name: A string starting with "*." (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name.

XN-Label: From RFC 5890 (https://tools.ietf.org/html/rfc5890): "The class of labels that begin with the prefix"xn--" (case independent), but otherwise conform to the rules for LDH labels."

1.6.2 ACRONYMS

CA	Certification Authority
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully-Qualified Domain Name
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
TN	Tunisia
TSP	Trust Service Provider
VOIP	Voice Over Internet Protocol

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

TunTrust makes the following available on its public repository at https://www.tuntrust.tn/repository:

- TunTrust CP/CPS;
- Subscriber contractual agreements (e.g: Subscriber Agreement, Application Forms, etc.);
- Audit Reports by Qualified Auditors;

- Certification Authority Certificates and related Authority Revocation Lists (ARLs);
- Certificate Revocation Lists (CRLs).

For further details regarding the publication of information refer to section 2.2.

TunTrust ensures that revocation data for issued Certificates and its Root Certificates are available in accordance with the CP/CPS.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

TunTrust conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates published at https://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

TunTrust publishes information mentioned in section 2.1 on its publicly accessible website https://www.tuntrust.tn/repository that is available on a 24x7 basis.

In addition, TunTrust publishes test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. These test Web pages are accessible at the following URLs:

- Valid Certificate: https://validovssl.tuntrust.tn/
- Revoked Certificate: https://revokedovssl.tuntrust.tn/
- Expired Certificate: https://expiredovssl.tuntrust.tn/

Prior to issuing SSL Certificates, TunTrust checks for CAA records for each dNSName in the subjectAltName extension of the Certificate to be issued as specified in RFC 8659 as per Section 4.2.4. TunTrust's CAA issuer domain is "tuntrust.tn".

2.3 TIME OR FREQUENCY OF PUBLICATION

TunTrust reviews its CP/CPS at least once every 366 days and makes appropriate changes so that TunTrust CA operation remains accurate, transparent and complies with requirements listed in Section 8 of this document. TunTrust CA closely monitors CA/Browser Forum ballots and updates to the Baseline Requirements and implements updates to TunTrust operations in a timely manner.

Revision Table in Section 1.2 indicates reviews and updates made to this CP/CPS by adding a dated changelog entry and incrementing the CP/CPS version number, even if no other changes are made to the document.

New or modified versions of this CP/CPS, Subscriber Agreements, or Relying Party agreements are published within seven days after approval.

Publication frequency of CRLs and frequency of updating OCSP records are specified in Sections 4.9.7 and 4.9.9.

2.4 ACCESS CONTROLS ON REPOSITORIES

Read only access to the repository is unrestricted. Logical and physical controls prevent unauthorized write access to repositories.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

The Subscriber is described in the Certificate by a Distinguished Name pursuant to the X.501 standard.

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

Any Fully-Qualified Domain Name (FQDN) which is embedded into a Certificate either as a DN component, or as a dnsName subjectAltName must conform to the standard semantics for DNS names described in RFC 1034. All DNS names embedded into an OV SSL Certificate issued by TunTrust is restricted by the ".tn" top-level domain for Tunisia and owned by entities operating under the Tunisian Jurisdiction.

Organizational names must be validated to be syntactically identical to an entry in the Tunisian National Registry of Enterprises (Registre National des Entreprises) as was used to validate the certificate request.

If the combination of names or the organization name by itself exceeds 64 characters, TunTrust abbreviates parts of the organization name, and/or omit non-material words in the organization name in such a way that the text in this field does not exceed the 64-character limit; provided that TunTrust checks this field in accordance with section 4.2.1 and a Relying Party will not be misled into thinking that they are dealing with a different organization.

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

TunTrust does not issue anonymous or pseudonymous Certificates.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

Fields contained in OV SSL Certificates are in compliance with this CP/CPS. In general, the rules for interpreting name forms can be found in International Telecommunication (ITU) and Internet Engineering Task Force (IETF) Standards, such as the ITU-T X.500 series of standards and applicable IETF RFCs.

3.1.5 UNIQUENESS OF NAMES

The full combination of the Subject Attributes (DN) is unique within the boundaries defined by this CP/CPS and conforms to all applicable X.509 standards for the uniqueness of names. The SerialNumber attribute guarantees the uniqueness of the DN in the Certificate.

3.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

TunTrust will issue certificates including trademarks only if the trademark is registered in the Tunisian National Register of Enterprises (Registre National des Entreprises). TunTrust will not issue certificates with trademarks that are not documented in the National Register of Enterprises.

3.2 INITIAL IDENTITY VALIDATION

TunTrust performs identification of the Applicant using any legal means of communication or investigation necessary to identify the Legal Entity and individual.

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

The Applicant provides a digitally signed PKCS#10 CSR to establish that it holds the private key corresponding to the public key to be included in an OV SSL Certificate. TunTrust parses the PKCS#10 CSR submitted by the Applicant and verifies that the Applicant's digital signature on the PKCS#10 was created by the private key corresponding to the public key in the PKCS#10 CSR.

3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

TunTrust issues OV SSL Certificates for public and private organizations under the Tunisian Jurisdiction and having a domain name under the ".tn" top-level domain.

TunTrust verifies the identity of the Applicant, and the authenticity of the Applicant Representative's certificate request using a verification process meeting the requirements of Section 3.2.2.1. TunTrust inspects any document relied upon for alteration or falsification.

3.2.2.1 IDENTITY

TunTrust verifies the existence and identity of the organization using the following methods:

- For Ministries and administrative public enterprises: TunTrust will obtain an excerpt from Official Gazette of Tunisia that proves the legal existence of the entity. Other information such as the address of the entity and the identity of the assigned responsible of the entity are verified based on other legal documents and official correspondences with the requesting agency or a superior government entity.
- For non-administrative public enterprises and private entities: TunTrust will obtain the information from the Tunisian National Register of Enterprises. The information extracted from the Tunisian National Register of Enterprises includes at a minimum the legal name, legal address, tax identification number, first name and last name of the legal representative.

Alternatively, TunTrust may verify the address, the phone number or email address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, Tunisia Yellow Pages or other form of identification that the CA determines to be reliable.

In order to validate the relationship of a physical person requesting an OV SSL certificate with the organization, the following information is required:

- The information in the National Identity Card (for Tunisians), obtained through a verification tool based on webservices of governmental entities that meet the requirements of section 3.2.2.7put at the disposal of the RA operator, or a copy of the passport or Tunisia residency card (for foreigners) of one of the physical persons who is a legal representative of the organization.

- The information in the National Identity Card (for Tunisians), obtained through a verification tool based on webservices of governmental entities that meet the requirements of section 3.2.2.7 put at the disposal of the RA operator, or a copy of the passport or Tunisia residency card (for foreigners) of the Certificate Manager.

3.2.2.2 DBA/TRADENAME

If the Subject Identity Information is to include a DBA or tradename, TunTrust verifies the Applicant's right to use the DBA/tradename using at least one of the following:

- A recent extract from the Tunisian National Register of Enterprises not older than 3 months;
- Communication with a government entity responsible for the management of such DBAs or trade names.

The registered DBA/tradename in official document must match the claimed DBA/tradename exactly.

3.2.2.3 VERIFICATION OF COUNTRY

TunTrust verifies that the organization is under the Tunisian jurisdiction. The country field is always set to Tunisia ISO format country code "TN". TunTrust does not issue SSL certificates to organizations that are not under the Tunisian Jurisdiction.

3.2.2.4 VALIDATION OF DOMAIN AUTHORIZATION OR CONTROL

TunTrust confirms that prior to issuance, TunTrust has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below. TunTrust does not issue certificates with a FQDN that contain "onion" as the rightmost Domain Label.

TunTrust maintains a record of which domain validation method, including relevant Baseline Requirements version number that was used to validate every domain.

Effective 2026-03-15: TunTrust performs DNSSEC validation back to the IANA DNSSEC root trust anchor on all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective. The DNS resolver used for all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective MUST:

- Perform DNSSEC validation using the algorithm defined in RFC 4035 Section 5; and
- Support NSEC3 as defined in RFC 5155; and
- Support SHA-2 as defined in RFC 4509 and RFC 5702; and
- Properly handle the security concerns enumerated in RFC 6840 Section 4.

Effective 2026-03-15:

For e-mail Domain Validation method described in section 3.2.2.4.4, TunTrust performs DNSSEC validation back to the IANA DNSSEC root trust anchor on all DNS CNAME, CAA, TXT queries attempting to obtain the Authorization Domain Name associated with the validation of domain authorization or control by the Primary Network Perspective.

TunTrust does not use local policy to disable DNSSEC validation. For all other DNS queries, DNSSEC validation back to the IANA DNSSEC root trust anchor SHOULD be performed and TunTrust SHOULD NOT use local policy to disable DNSSEC validation. For all other Domain Validation methods, DNSSEC validation back to the IANA DNSSEC root trust anchor MUST be performed on all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective and TunTrust MUST NOT use local policy to disable DNSSEC validation on any DNS query associated with the validation of domain authorization or control.

DNSSEC validation back to the IANA DNSSEC root trust anchor is considered outside the scope of self-audits performed to fulfill the requirements in Section 8.7.

DNSSEC validation back to the IANA DNSSEC root trust anchor is considered outside the scope of the logging requirements of Section 5.4.1.

3.2.2.4.1 Validating the Applicant as a Domain Contact

TunTrust does not use this method.

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

Effective 16 December 2024, TunTrust does not use this method.

3.2.2.4.3 Phone Contact With Domain Contact

TunTrust does not use this method.

3.2.2.4.4 Email to a Constructed Email To address

TunTrust confirms the Applicant's control over the FQDN or Wildcard Domain names by:

1. sending an email to one or more addresses created by using ‘admin’, ‘administrator’, 'webmaster’, ’hostmaster’, or ‘postmaster’ as the local part, followed by the at-sign (“@”), followed by an Authorization Domain Name,
2. including a Random Value in the email, and
3. receiving a confirming response utilizing the Random Value.

This email provides a confirmation link with a Random Value that the Applicant must follow to confirm control over the domain name.

Each email may confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed.

The email with no content and no recipient modification may be re-sent in its entirety, including the re-use of the Random Value. The Random Value remains valid for use in a confirming response for no more than 30 days from its creation.

Once the FQDN has been validated using this method, TunTrust may also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.5 Domain Authorization Document

TunTrust does not use this method.

3.2.2.4.6 Agreed-Upon Change to Website

TunTrust does not use this method.

3.2.2.4.7 DNS Change

TunTrust confirms the Applicant’s control over the FQDN by confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT or CAA record for either

1. 1. an Authorization Domain Name; or

2. 2. an Authorization Domain Name that is prefixed with a Domain Label that begins with an underscore character.

If a Random Value is used, TunTrust provides a Random Value unique to the Certificate request and does not use the Random Value after:

1. 30 days; or
2. if the Applicant submitted the Certificate request, the time frame permitted for reuse of validated information relevant to the Certificate (such as in Section 4.2.1 of the Baseline Requirements).

TunTrust implements Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To be considered corroborating, a Network Perspective MUST observe the same challenge information (i.e., Random Value or Request Token) as TunTrust's Primary Network Perspective.

Note: Once the FQDN has been validated using this method, TunTrust may also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.8 IP Address

TunTrust does not use this method.

3.2.2.4.9 Test Certificate

TunTrust does not use this method.

3.2.2.4.10 TLS Using a Random Value

TunTrust does not use this method.

3.2.2.4.11 Any Other Method

TunTrust does not use any other method.

3.2.2.4.12 Validating Applicant as a Domain Contact

TunTrust does not use this method.

3.2.2.4.13 Email to DNS CAA Contact

TunTrust does not use this method.

3.2.2.4.14 Email to DNS TXT Contact

TunTrust does not use this method.

3.2.2.4.15 Phone Contact with Domain Contact

TunTrust does not use this method.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

TunTrust does not use this method.

3.2.2.4.17 Phone Contact with DNS TXT Record Phone Contact

TunTrust does not use this method.

3.2.2.4.18 Agreed-Upon Change to Website v2

TunTrust does not use this method.

3.2.2.4.19 Agreed-Upon Change to Website - ACME

Confirming the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in RFC 8555, Section 8.3. The following are additive requirements to RFC 8555.

TunTrust MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The token (as defined in RFC 8555, Section 8.3) MUST NOT be used for more than 30 days from its creation.

If TunTrust follows redirects, the following apply:

1. Redirects MUST be initiated at the HTTP protocol layer. Redirects MUST be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3. Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.
2. Redirects MUST be to resource URLs with either the "http" or "https" scheme.
3. Redirects MUST be to resource URLs accessed via Authorized Ports.

Except for Onion Domain Names, TunTrust implements Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. Random Value or Request Token) as the Primary Network Perspective.

Note: TunTrust does not issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless TunTrust performs separate validations for each of those other FQDN using authorized methods. This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.20 TLS Using ALPN

TunTrust does not use this method.

3.2.2.4.21 DNS Labeled with Account ID - ACME

TunTrust does not use this method.

3.2.2.4.22 DNS TXT Record with Persistent Value

TunTrust does not use this method.

3.2.2.5 Authentication for an IP Address

TunTrust does not issue certificates with IP addresses.

3.2.2.6 Wildcard domain validation

If a Wildcard Domain Name is to be included in a Certificate, then TunTrust issuing CAs remove "`*.`" from the left-most portion of the Wildcard Domain Name to yield the corresponding FQDN. TunTrust issuing CAs may prune zero or more Domain Labels of the FQDN from left to right until encountering a Base Domain Name and

may use any one of the values that were yielded by pruning (including the Base Domain Name itself) for the purpose of domain validation.

Before issuing a Wildcard Certificate, TunTrust issuing CAs follow an internal documented procedure that determines if the FQDN portion of any Wildcard Domain Name in the Certificate is "registry-controlled"[1] or is a "public suffix" under the ".tn" domain.

If the FQDN portion of any Wildcard Domain Name is "registry-controlled" or is a "public suffix", the TunTrust issuing CAs refuse issuance unless the Applicant proves its rightful control of the entire Domain Namespace.

3.2.2.7 DATA SOURCE ACCURACY

TunTrust uses Tunisian governmental entities as data sources and third party databases sourced from Tunisian governmental entities and regularly updated such that TunTrust considers it a reliable data source.

Before relying on any data provided, TunTrust will verify the following attributes:

- The age of the information provided,
- The frequency of updates to the information source,
- The data provider and purpose of the data collection,
- The public accessibility of the data availability, and
- The relative difficulty in falsifying or altering the data.

3.2.2.8 CAA RECORDS

Refer to Section 4.2.2.1 for CAA record processing requirements.

3.2.2.8.1 DNSSEC VALIDATION OF CAA RECORDS

Refer to Section 4.2.2.1.3 for DNSSEC validation of CAA record processing requirements.

3.2.2.9 MULTI-PERSPECTIVE ISSUANCE CORROBORATION

Multi-Perspective Issuance Corroboration attempts to corroborate the determinations (i.e., domain validation pass/fail, CAA permission/prohibition) made by the Primary Network Perspective from multiple remote Network Perspectives before Certificate issuance. This process can improve protection against equally-specific prefix Border Gateway Protocol (BGP) attacks or hijacks.

TunTrust MAY use either the same set, or different sets of Network Perspectives when performing Multi-Perspective Issuance Corroboration for the required 1) Domain Authorization or Control and 2) CAA Record checks.

1Determination of what is "registry-controlled" versus the registerable portion of a Country Code Top-Level Domain Namespace is not standardized at the time of writing and is not a property of the DNS itself. Current best practice is to consult a "public suffix list" such as Public Suffix List (PSL) , and to retrieve a fresh copy regularly. If using the PSL, a CA SHOULD consult the "ICANN DOMAINS" section only, not the "PRIVATE DOMAINS" section. The PSL is updated regularly to contain new gTLDs delegated by ICANN, which are listed in the "ICANN DOMAINS" section. A CA is not prohibited from issuing a Wildcard Certificate to the Registrant of an entire gTLD, provided that control of the entire namespace is demonstrated in an appropriate way.

The set of responses from the relied upon Network Perspectives MUST provide TunTrust with the necessary information to allow it to affirmatively assess:

- a. the presence of the expected 1) Random Value, 2) Request Token, 3) IP Address, or 4) Contact Address, as required by the relied upon validation method specified in Sections 3.2.2.4 and 0; and

- b. TunTrust's authority to issue to the requested domain(s), as specified in Section 3.2.2.8.

Section 3.2.2.4 and Section 3.2.2.5 describe the validation methods that require the use of Multi-Perspective Issuance Corroboration and how a Network Perspective can corroborate the outcomes determined by the Primary Network Perspective.

Results or information obtained from one Network Perspective is NOT reused or cached when performing validation through subsequent Network Perspectives (e.g., different Network Perspectives cannot rely on a shared DNS cache to prevent an adversary with control of traffic from one Network Perspective from poisoning the DNS cache used by other Network Perspectives). The network infrastructure providing Internet connectivity to a Network Perspective MAY be administered by the same organization providing the computational services required to operate the Network Perspective. All communications between a remote Network Perspective and TunTrust takes place over an authenticated and encrypted channel relying on modern protocols (e.g., over HTTPS).

A Network Perspective MAY use a recursive DNS resolver that is NOT co-located with the Network Perspective. However, the DNS resolver used by the Network Perspective MUST fall within the same Regional Internet Registry service region as the Network Perspective relying upon it. Furthermore, for any pair of DNS resolvers used on a Multi-Perspective Issuance Corroboration attempt, the straight-line distance between the two DNS resolvers MUST be at least 500 km. The location of a DNS resolver is determined by the point where unencapsulated outbound DNS queries are typically first handed off to the network infrastructure providing Internet connectivity to that DNS resolver.

TunTrust MAY immediately retry Multi-Perspective Issuance Corroboration using the same validation method or an alternative method (e.g., TunTrust can immediately retry validation using "DNS Change" if "Agreed-Upon Change to Website - ACME" does not corroborate the outcome of Multi-Perspective Issuance Corroboration). When retrying Multi-Perspective Issuance Corroboration, TunTrust does NOT rely on corroborations from previous attempts. There is no stipulation regarding the maximum number of validation attempts that may be performed in any period of time.

The "Quorum Requirements" Table describes quorum requirements related to MultiPerspective Issuance Corroboration. If the CA does NOT rely on the same set of Network Perspectives for both Domain Authorization or Control and CAA Record checks, the quorum requirements MUST be met for both sets of Network Perspectives (i.e.,the Domain Authorization or Control set and the CAA record check set). Network Perspectives are considered distinct when the straight-line distance between them reside in is at least 500 km. Network Perspectives are considered "remote" when they are distinct from the Primary Network Perspective and the other Network Perspectives represented in a quorum.

TunTrust MAY reuse corroborating evidence for CAA record quorum compliance for a maximum of 398 days. After issuing a Certificate to a domain, remote Network Perspectives MAY omit retrieving and processing CAA records for the same domain or its subdomains in subsequent Certificate requests from the same Applicant for up to a maximum of 398 days.

Table 4: Quorum Requirements

# of Distinct Remote Network Perspectives Used	# of Allowed non-Corroborations
2-5	1
6+	2

Remote Network Perspectives performing Multi-Perspective Issuance Corroboration:

MUST:

- Network Hardening:
  - Rely upon networks (e.g., Internet Service Providers or Cloud Provider Networks) implementing measures to mitigate BGP routing incidents in the global Internet routing system for providing internet connectivity to the Network Perspective.

SHOULD:

- Facility & Service Provider Requirements:
  - Be hosted from an ISO/IEC 27001 certified facility or equivalent security framework independently audited and certified or reported.
  - Rely on services covered in one of the following reports: System and Organization Controls 2 (SOC 2), ISAE 3000, ENISA 715, FedRAMP Moderate, C5:2020, CSA STAR CCM, or equivalent services framework independently audited and certified or reported.
- Vulnerability Detection and Patch Management:
  - Implement intrusion detection and prevention controls to protect against common network and system threats.
  - Document and follow a vulnerability correction process that addresses the identification, review, response, and remediation of vulnerabilities.
  - Undergo or perform a Vulnerability Scan at least every three (3) months.
  - Undergo a Penetration Test on at least an annual basis.
  - Apply recommended security patches within six (6) months of the security patch's availability, unless the CA documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.

- System Hardening:
  - Disable all accounts, applications, services, protocols, and ports that are not used.
  - Implement multi-factor authentication for all user accounts.

- Network Hardening:
  - Configure each network boundary control (firewall, switch, router, gateway, or other network control device or system) with rules that support only the services, protocols, ports, and communications identified as necessary to its operations.

- Rely upon networks (e.g., Internet Service Providers) that: 1) use mechanisms based on Secure Inter-Domain Routing (RFC 6480), for example, BGP Prefix Origin Validation (RFC 6811), 2) make use of other non-RPKI route-leak prevention mechanisms (such as RFC 9234), and 3) apply current best practices described in BCP 194. While It is RECOMMENDED that under normal operating conditions Network Perspectives performing Multi-Perspective Issuance Corroboration forward all Internet traffic via a network or set of networks that filter RPKI-invalid BGP routes as defined by RFC 6811, it is NOT REQUIRED.

Beyond the above considerations, computing systems performing Multi-Perspective Issuance Corroboration are considered outside of the audit scope described in Section 8 of the Baseline Requirements.

Phased Implementation Timeline:

- Effective 2025-03-15, TunTrust implements Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives. TunTrust MAY proceed with certificate issuance if the number of remote Network Perspectives that do not corroborate the determinations made by the Primary Network Perspective ("non-corroborations") is greater than allowed in the Quorum Requirements table.

- Effective 2025-09-15, TunTrust implements Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives. TunTrustensures that the requirements defined in Quorum Requirements Table are satisfied. If the requirements are not satisfied, then TunTrustMUST NOT proceed with issuance of the Certificate.

- Effective 2026-03-15, TunTrust implements Multi-Perspective Issuance Corroboration using at least three (3) remote Network Perspectives. TunTrust MUST ensure that the requirements defined in Quorum Requirements Table are satisfied, and the remote Network Perspectives that corroborate the Primary Network Perspective fall within the service regions of at least two (2) distinct Regional Internet Registries. If the requirements are not satisfied, then TunTrust MUST NOT proceed with issuance of the Certificate.

- Effective 2026-06-15, TunTrust implements Multi-Perspective Issuance Corroboration using at least four (4) remote Network Perspectives. TunTrust MUST ensure that the requirements defined in Quorum Requirements Table are satisfied, and the remote Network Perspectives that corroborate the Primary Network Perspective fall within the service regions of at least two (2) distinct Regional Internet Registries. If the requirements are not satisfied, then TunTrust MUST NOT proceed with issuance of the Certificate.

- Effective 2026-12-15, TunTrust implements Multi-Perspective Issuance Corroboration using at least five (5) remote Network Perspectives. TunTrust ensures that the requirements defined in Quorum Requirements Table are satisfied, and the remote Network Perspectives that corroborate the Primary Network Perspective fall within the service regions of at least two (2) distinct Regional Internet Registries. If the requirements are not satisfied, then TunTrust MUST NOT proceed with issuance of the Certificate.

3.2.3 AUTHENTICATION OF INDIVIDUAL IDENTITY

TunTrust does not issue OV SSL certificates to natural persons. However, as part of the certificate application process, TunTrust will verify the identity of the Certificate Manager and the legal representative of the organization as detailed in Section 3.2.2.1.

The Certificate Manager is either the Legal Representative of the entity or a natural person formally designated by the Legal Representative. The designation of a Certificate Manager is performed simultaneously with the submission of the OV SSL Certificate Application Form.

As mentioned in Section 4.1.2, the Certificate Application Form is signed by : (i) the Legal Representative to mandate the future Certificate Manager and (ii) the future Certificate Manager to accept this role and the Subscriber Agreement.

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

Unverified information is never included in TunTrust end entities Certificates. All Subscriber information included in Certificates are duly verified.

3.2.5 VALIDATION OF AUTHORITY

This step is performed simultaneously with the validation of the identity of the Legal Representative and of the Certificate Manager. As mentioned in Section 3.2.3, the certificate application form is signed by the legal representative of the entity and the certificate manager and each of them must provide a copy of his or her ID. Signatures of the Legal Representative and Certificate Manager must be a legally valid and contain an enforceable seal or handwritten signature or be a legally valid and enforceable electronic signature.

In addition, TunTrust uses a Reliable Method of Communication derived from the verification process described in section 3.2.2.1 to establish the authenticity of the certificate request directly with the Applicant Legal Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that TunTrust deems appropriate.

3.2.6 CRITERIA FOR INTEROPERATION

TunTrust does not have any Cross-Certified Subordinate CA Certificates with other CAs.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

Not Applicable. TunTrust does not support rekey.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

Not Applicable. TunTrust does not support re-key.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests are authenticated to ensure they emanate from authorized persons. The process how the revocation request can be submitted is described in Section 4.9.3.

TunTrust may also perform revocation on behalf of Subscribers in accordance with the requirements of the applicable Subscriber Agreement. Examples of reasons for revocation include a breach of the Subscriber Agreement or non-payment of applicable fees.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

OV SSL certificates applications can only be submitted by Applicant under the Tunisian Jurisdiction. Applicants must comply with provisions set within the registration forms and processes, this CP/CPS and the Subscriber Agreement.

TunTrust maintains an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. TunTrust uses this information to identify individuals from whom and entities from which it will not accept Certificate applications.

In addition, other external sources such as government denied lists or internationally recognized denied persons lists which are applicable to the jurisdictions in which TunTrust operates are used to screen out unwanted Applicants.

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

TunTrust makes available to Applicants all required Application forms as well as all applicable Subscriber Agreements: (i) on its public repository at https://www.tuntrust.tn/repository, (ii) by email to tuntrust@tuntrust.tn, (iii) and within its headquarters (see Section 1.5.2).

Prior to the issuance of a Certificate, TunTrust obtains a dully filled and signed Application Form that falls into five parts as described hereafter:

- Part 1 : Applicant details including legal name, tax identification number, a telephone number, fax number, email address, and postal delivery address,
- Part 2 : Legal Representative details including full name, ID Number, telephone number and email address
- Part 3 : Certificate Manager details including full name, ID Number, telephone number and email address
- Part 4 : Certificate type; Certificate Validity, FQDN Names to embed into the SSL Certificate
- Part 5 : Signature of the Legal Representative and the Certificate Manager by which they confirm their acceptance and compliance with the Subscriber Agreement

The Applicant commits to providing a current, genuine and complete certificate request and all evidence requested by TunTrust. The paper Application, with the Applicant wet seal and handwritten signatures of the Applicant's legal representative and the Certificate Manager, must be physically submitted to TunTrust RA. Applicant may submit electronic Application Form with the digital signature of the Applicant Legal Representative and the Certificate Manager. The digital signatures of Legal Representative and Certificate Manager must be compliant withthe Tunisian Law related to digital signature.

The Applicant generates the key pair by itself and creates a Certificate Signing Request (CSR) as to prove that the private key belongs to itself and sends it to TunTrust RA from the email address used to verify domain

control or provides it to TunTrust RA operator on a hardware device (CD, USB Token). The Applicant is responsible for taking all required measures for protecting confidentiality and integrity of its private key.

TunTrust's responsibility is to verify and to validate the information supplied. This will be done in compliance with the practices stated in this CP/CPS and by strictly following the TunTrust registration procedures and the applicable national laws.

TunTrust guarantees that all required verifications have been performed prior to successful registration leading to Certificate issuance and that all certificate requests submitted to the Issuing CAs are complete, accurate, valid and duly authorized. It also guarantees the accuracy of all information contained in the Certificate.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Applications for OV SSL Certificates shall be submitted by the legal representative of the organization who owns the Domain Name.

OV SSL Certificate application includes the following:

- Order Form including the Subscriber Agreement as described in Section 4.1.
- Documents proving the legal existence of the Applicant if the Organization does not have a Tunisian National Register of Enterprises (Section 3.2.2),
- Copy of the ID of the legal representative if he/she does not have the Tunisian nationality (passport or Tunisia residency card),
- Copy of the ID of the Certificate Manager if he/she does not have the Tunisian nationality (passport or Tunisia residency card),
- The Certificate Signing Request (CSR) that includes at least one Fully-Qualified Domain Name to be included in the Certificate's subjectAltName extension.

The following verification tasks are performed by TunTrust's RA:

- Validation of the identity and the legal existence of the Applicant (Section 3.2.2) : The Applicant must be a legal entity under the Tunisian Jurisdiction;
- Validation of the identity of the legal representative and the Certificate Manager (section 3.2.2);
- Validation of domain control (section 3.2.2.4);
- Assurance that the certificate request does not fall into high risk or blacklisted certificate requests (Section 3.2.2.9 and Section 4.2.1);
- Verification of CAA records for each dNSName in the subjectAltName extension of the Certificate to be issued (Section 3.2.2.8).

TunTrust does not re-use previous validation information. Each certificate application must go through all validation functions described in section 3.2. End-user Certificate validity is specified in Section 6.3.2.

TunTrust maintains an internal database of all previously revoked SSL Certificates and previously rejected Certificate requests due to suspected phishing or other fraudulent usage or concerns. TunTrust uses this information to identify subsequent suspicious certificate requests. If a new request for a previously denied SSL Certificate is made, the application will be flagged and brought to the attention of management to complete further internal verification and final decision.

TunTrust develops, maintains, and implements documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified by doing the following:

- TunTrust maintains a list of prior high-risk requests specifying current high-risk Domain Names. This list is used by TunTrust to identify potential risks.
- TunTrust also uses an automated Domain name permutation engine for detecting potential typo squatting and phishing threat.

Application with potential High Risk will be flagged and brought to the attention of management to complete further internal verification and final decision.

For validation of Domain Names and IP Addresses according to Section 3.2.2.4 and Section, any data, document, or completed validation used MUST be obtained within the maximum number of days prior to issuing the Certificate, as defined in the following table:

Certificate issued on or after	Certificate issued before	Maximum data reuse period
	2026-03-15	398 days
2026-03-15	2027-03-15	200 days
2027-03-15	2029-03-15	100 days
2029-03-15		10 days

TABLE 1 : DOMAIN NAME AND IP ADDRESS VALIDATION DATA REUSE PERIODS

4.2.2 Approval Or Rejection Of Certificate Applications

TunTrust will approve or reject an Applicant's Certificate request based upon the Applicant meeting the requirements of this CP/CPS and all applicable laws and regulations.

TunTrust rejects any certificate application that TunTrust cannot verify. TunTrust does not issue Certificates for Domain Names that are not under the ".tn" top-level domain. TunTrust does not issue certificates containing Internal Names or Reserved IP Addresses, as such names cannot be validated according to Section 3.2.2.4 or Section 3.2.2.5

TunTrust, in its sole discretion, may reject a Certificate Application, and may refuse to issue a Certificate, without incurring any liability for loss or damages arising out of such refusal. TunTrust reserves the right not to disclose reasons for such a refusal. Applicants whose applications have been rejected may subsequently re-apply.

TunTrust, at its sole discretion not to be unreasonably withheld, may override any decision to Approve Applicant's Certificate request.

4.2.2.1 CAA RECORD PROCESSING

As part of the Certificate issuance process, TunTrust retrieves and processes CAA records in accordance with RFC 8659 for each `dNSName` in the `subjectAltName` extension that does not contain an Onion Domain Name.

These practices are described in Section 4.2 of TunTrust Certificate Policy and/or Certification PracticeStatement, including specifying the set of Issuer Domain Names that the CA recognizes in CAA “issue” or “issuewild” records as permitting it to issue.

Some methods relied upon for validating the Applicant’s ownership or control of the subject domain(s) (see Section 3.2.2.4) or IP address(es) (see Section 0) to be listed in a Certificate require CAA records to be retrieved and processed from additional remote Network Perspectives before Certificate issuance (see Section 3.2.2.9). To corroborate the Primary Network Perspective, a remote Network Perspective’s CAA check response MUST be interpreted as permission to issue, regardless of whether the responses from both Perspectives are byte-for-byte identical. Additionally, TunTrust MAY consider the response from a remote Network Perspective as corroborating if one or both of the Perspectives experience an acceptable CAA record lookup failure, as defined in this section.

TunTrust MAY check CAA records at any other time.

When processing CAA records, TunTrust processes the issue, issuewild, and iodef property tags as specified in RFC 8659, although they are not required to act on the contents of the iodef property tag. Additional property tags MAY be supported, but MUST NOT conflict with or supersede the mandatory property tags set out in this document. TunTrust respects the critical flag and not issue a certificate if it encounters an unrecognized property tag with this flag set.

If the TunTrust issues a certificate after processing a CAA record, it MUST do so within the TTL of the CAA record, or 8 hours, whichever is greater

RFC 8659 requires that CAs "MUST NOT issue a certificate unless TunTrust determines that either (1) the certificate request is consistent with the applicable CAA RRset or (2) an exception specified in the relevant CP or CPS applies." For issuances conforming to the Baseline Requirements, TunTrust does not rely on any exceptions specified in this CP/CPS unless they are one of the following:

- CAA checking is optional for certificates for which a Certificate Transparency Precertificate (see Section 7.1.2.9) was created and logged in at least two public logs, and for which CAA was checked at time of Precertificate issuance.
- CAA checking is optional for Certificates issued by a Technically Constrained Subordinate CA Certificate as set out in Section 7.1.2.3 or Section 7.1.2.5, where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant.

TunTrust is permitted to treat a record lookup failure as permission to issue if:

- the failure is outside TunTrust's infrastructure; and
- the lookup has been retried at least once; and

- the domain's zone does not have a DNSSEC validation chain to the ICANN root.

TunTrust documents potential issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CA/Browser Forum on the circumstances, and endeavors to dispatch reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s), if present. TunTrust is not expected to support URL schemes in the iodef record other than mailto: or https:.

4.2.2.1.1 CAA Multi-Perspective Issuance Corroboration

Some methods relied upon for validating the Applicant's ownership or control of the subject domain(s) (see Section 3.2.2.4) or IP address(es) (see Section 3.2.2.5) to be listed in a certificate require CAA records to be retrieved and processed from additional remote Network Perspectives before Certificate issuance (see Section 3.2.2.9). To corroborate the Primary Network Perspective, a remote Network Perspective's CAA check response MUST be interpreted as permission to issue, regardless of whether the responses from both Perspectives are byte-for-byte identical. Additionally, a CA MAY consider the response from a remote Network Perspective as corroborating if one or both of the Perspectives experience an acceptable CAA record lookup failure, as defined in Section 4.2.2.1.

4.2.2.1.2 CAA Parameters

When processing CAA records, TunTrust SHOULD process the accounturi and validationmethods parameters as specified in RFC 8657. Effective 2027-03-15, when processing CAA records, CAs MUST process the accounturi and validationmethods parameters as specified in RFC 8657.

In addition, Effective 2027-03-15: - If TunTrust does not identify the Subscriber account via an ACME Account URL as described in RFC 8555, the CA MUST define the supported format of the accounturi in Section 4.2 of their CP and/or CPS, and SHOULD comply with the 'acct' URI scheme defined in RFC 7565. - For certificate requests made using the ACME protocol, TunTrust MAY permit the 'accounturi' parameter to identify a primary organizational account (the "Parent Account"). As an explicit exception to Section 3 of RFC 8657, TunTrust MAY issue a certificate requested by a different account (the "Subordinate ACME Account") if and only if TunTrust ensures all of the following:

1. TunTrust maintains an internal, auditable mapping that binds the Subordinate ACME Account to the Parent Account identified by the 'accounturi'.

2. TunTrust has cryptographically or administratively verified that the Parent Account explicitly authorized the Subordinate ACME Account to obtain certificates under this mapping.

3. TunTrust retains audit logs demonstrating this authorization and mapping for the standard data retention period required by these Requirements. - If TunTrust supports domain validation methods that are not registered in the IANA ACME Validation Methods registry, TunTrust MUST interpret and process validationmethods labels formed by concatenating the string 'ca-tbr-' with the BR 3.2.2.4 subsection number, e.g. 'ca-tbr-7' represents the DNS method described in TLS BR 3.2.2.4.7. If a CA performs domain validation using a mechanism that can be represented by multiple labels (e.g. 'http-01' and 'ca-tbr-19'), TunTrust SHOULD accept any of the labels as granting permission to issue. - The canonical representation of validationmethods labels is lowercase letters. However, TunTrust MAY perform case insensitive matching of labels. If the CA does perform case insensitive matching of labels, this practice MUST be documented in their CP and/or CPS.

4.2.2.1.3 DNSSEC Validation of CAA Records

Effective 2026-03-15: TunTrust performs DNSSEC validation back to the IANA DNSSEC root trust anchor

on all DNS queries associated with CAA record lookups performed by the Primary Network Perspective. The DNS resolver used for all DNS queries associated with CAA record lookups performed by the Primary Network Perspective MUST:

• Perform DNSSEC validation using the algorithm defined in RFC 4035 Section 5; and

• Support NSEC3 as defined in RFC 5155; and

• Support SHA-2 as defined in RFC 4509 and RFC 5702; and

• Properly handle the security concerns enumerated in RFC 6840 Section 4.

Effective 2026-03-15: TunTrust does not use local policy to disable DNSSEC validation on any DNS query associated CAA record lookups.

Effective 2026-03-15: DNSSEC-validation errors observed by the Primary Network Perspective (e.g., SERVFAIL) MUST NOT be treated as permission to issue.

TunTrust MAY perform DNSSEC validation back to the IANA DNSSEC root trust anchor on all DNS queries associated with CAA record lookups performed by Remote Network Perspectives as part of Multi-Perspective Issuance Corroboration.

DNSSEC validation back to the IANA DNSSEC root trust anchor is considered outside the scope of self-audits performed to fulfill the requirements in Section 8.7.

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

Under normal circumstances, TunTrust confirms Certificate application information and issues a Certificate within seven working days as established by Tunisian national law.

4.2.4 CERTIFICATE AUTHORITY AUTHORISATION (CAA)

Prior to issuing SSL Certificates, TunTrust checks for CAA records for each dNSName in the subjectAltName extension of the Certificate to be issued as specified in RFC 8659. TunTrust's CAA issuer domain is "tuntrust.tn.". The following cases do not allow TunTrust to authorize the issuance of the certificate:

- The CAA DNS field is present, it contains an "issue" or "issuewild" tag and does not list TunTrust.tn as an authorized Certificate Authority;
- The CAA DNS field is present, it is designated as "critical" and the tag used is not supported by the CA (it is not an "issue" or "issuewild" tag);
- The zone is validly DNSSEC-signed and our DNS query times out.

If any of these cases are encountered, the certificate request is automatically blocked and the applicant is notified by email of the need to update the associated DNS records.

TunTrust:

- Caches CAA records for reuse for up to 8 hours
- Supports the issue and issuewild CAA tags
- Processes but does not act on iodef property tag (i.e., TunTrust does not dispatch reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s))
- Does not support any additional property tags.

TunTrust may not check CAA records for Certificates for which a Certificate Transparency pre-Certificate was created and logged in at least two public logs, and for which CAA was checked. No other CAA checking exceptions are applied.

TunTrust treats a record lookup failure as permission to issue if:

- The failure is outside TunTrust 's infrastructure; and
- The lookup has been retried at least once; and
- The domain's zone does not have a DNSSEC validation chain to the ICANN root.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

4.3.1.1 MANUAL AUTHORIZATION OF CERTIFICATE ISSUANCE FOR ROOT CAS

Upon receipt of an approved Certificate signing request, TunTrust CAs proceeds to the Certificate issuance process.

Certificate issuance by TunTrust CAs requires a Tuntrust RA operator in a Trusted Role authorized by TunTrust to deliberately issue a direct command in order for TunTrust CAs to perform a certificate signing operation. The RA operators accounts capable of causing certificate issuance or performing Registration Authority functions are enforced with multi-factor authentication (certificate in cryptographic token + PIN code). Technical controls are operated by TunTrust in order to restrict certificate issuance through accounts to a limited set of pre-approved email addresses. Each issuance is logged with the identity of the TunTrust RA operator issuing the certificate and the action is logged in the CA audit log.

Databases and CA processes occurring during certificate issuance are protected from unauthorized modification. After issuance is complete, the certificate is stored in a database and sent to the Subscriber.

4.3.1.2 LINTING OF TO-BE-SIGNED CERTIFICATE CONTENT

Due to the complexity involved in implementing Certificate Profiles that conform to the Base Requirements, it is considered best practice for the CA to implement a Linting process to test the technical conformity of each to-be-signed artifact prior to signing it. When a Precertificate has undergone Linting, it is not necessary for the corresponding to-be-signed Certificate to also undergo Linting, provided that the CA has a technical control to verify that the to-be-signed Certificate corresponds to the to-be-signed Precertificate in the manner described by RFC 6962, Section 3.2.

TunTrust CA uses an automated issuance process that integrates pre-issuance linting tools, kept up-to-date, which can check a tbsCertificate (To Be Signed Certificate - the certificate complete except for the signature) for a large number of standards violations (Baseline Requirements, RFCs, etc.). Certificate issuance is held up for manual review if a linting error or warning is found. The linting error is flagged and brought to the attention of management to complete further internal verification and final decision on the certificate issuance.

TunTrust uses the Linting tools that have been widely adopted by the industry (see https://cabforum.org/resources/tools/).

TunTrust will contribute, when possible, to open-source Linting projects, such as by:

- creating new or improving existing lints,
- reporting potentially inaccurate linting results as bugs,
- notifying maintainers of Linting software of checks that are not covered by existing lints,
- updating documentation of existing lints, and
- generating test certificates for positive/negative tests of specific lints.

4.3.1.3 Linting of issued Certificates

TunTrust may use a Linting process to test each issued Certificate.

4.3.2 Notification to Subscriber by the CA of issuance of Certificate

The Applicant will be notified that the Certificate is issued via the Certificate Manager email address that was supplied by the Subscriber during the enrollment process and will be provided with appropriate instructions on how to obtain the Certificate. If the Certificate is presented to the Subscriber immediately, special notification may not be necessary.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

A Subscriber that accepts a Certificate warrants to TunTrust, that all information supplied in connection with the application process and all information included in the Certificate issued to them is true, complete, and not misleading.

Without limitation to the generality of the foregoing, the use of a Certificate signifies acceptance by that Subscriber of this CP/CPS and Subscriber Agreement (as the same may, from time to time, be amended or supplemented) by which they irrevocably agree to be bound.

If the subscriber is not satisfied with the details contained within the certificate, he or she must email assistance@tuntrust.tn explaining why the certificate is not being accepted. This communication must take place within 30 days of issuance.

Certificates are considered accepted 30 days after the Certificate's issuance, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.4.2 Publication of the Certificate by the CA

Refer to Section 2.1.

4.4.3 Notification of Certificate issuance by the CA to other entities

Other than Certificate Transparency publication, TunTrust does not notify other entities of certificate issuance.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

Subscribers have to protect their Private Key to avoid disclosure to third parties. TunTrust provides a Subscriber Agreement which highlights the obligations of the Subscriber with respect to Private Key protection.

Subscribers are bound to use the Certificate for its lawful and intended purposes only.

At the end of the useful life of a Private Key, Subscribers must securely delete the Private Key and any fragments that it has been split into for the purposes of backup.

4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

Within this CP/CPS, TunTrust provides the conditions under which Certificates may be relied upon by Relying Parties including the appropriate Certificate services available to verify Certificate validity such as CRL and/or OCSP.

In order to be a Relying Party, a Party seeking to rely on a Certificate issued by TunTrust CA agrees to and accepts the Relying Party Agreement available at https://www.tuntrust.tn/repository by querying the existence or validity of; or by seeking to place or by placing reliance upon a Certificate.

Relying Parties are obliged to seek further independent assurances before any act of reliance is deemed reasonable and at a minimum must assess:

- The appropriateness of the use of the Certificate for any given purpose and that the use is not prohibited by this CP/CPS,
- That the Certificate is being used in accordance with its Key-Usage field extensions,
- That the Certificate is valid at the time of reliance by reference to OCSP or CRL Checks.

4.6 CERTIFICATE RENEWAL

Certificate renewal means the issuance of a new Certificate without changing the Public Key or any other information in the Certificate. Certificate renewal is not supported by TunTrust.

4.6.1 CIRCUMSTANCES FOR CERTIFICATE RENEWAL

Not Applicable. Certificate renewal is not supported by TunTrust.

4.6.2 WHO MAY REQUEST RENEWAL

Not Applicable. Certificate renewal is not supported by TunTrust.

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

Not Applicable. Certificate renewal is not supported by TunTrust.

4.6.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Not Applicable. Certificate renewal is not supported by TunTrust.

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

Not Applicable. Certificate renewal is not supported by TunTrust.

4.6.6 PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA

Not Applicable. Certificate renewal is not supported by TunTrust.

4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Not Applicable. Certificate renewal is not supported by TunTrust.

4.7 CERTIFICATE RE-KEY

Certificate re-key means the issuance of a new certificate with a new public key, but with the same subject identity information. TunTrust does not support re-key.

4.7.1 CIRCUMSTANCE FOR CERTIFICATE RE-KEY

Not Applicable. TunTrust does not support re-key.

4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

Not Applicable. TunTrust does not support re-key.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

Not Applicable. TunTrust does not support re-key.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Not Applicable. TunTrust does not support re-key.

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

Not Applicable. TunTrust does not support re-key.

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

Not Applicable. TunTrust does not support re-key.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Not Applicable. TunTrust does not support re-key.

4.8 CERTIFICATE MODIFICATION

Certificate modification is the process through which a Subscriber requests a Certificate with modified subject information. TunTrust considers such request as an initial registration request. The requester is therefore required to start a new Certificate request.

4.8.1 CIRCUMSTANCES FOR CERTIFICATE MODIFICATION

Not Applicable. TunTrust does not support Certificate modification.

4.8.2 WHO MAY REQUEST CERTIFICATE MODIFICATION

Not Applicable. TunTrust does not support Certificate modification.

4.8.3 PROCESSING CERTIFICATE MODIFICATION REQUESTS

Not Applicable. TunTrust does not support Certificate modification.

4.8.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Not Applicable. TunTrust does not support Certificate modification.

4.8.5 CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE

Not Applicable. TunTrust does not support Certificate modification.

4.8.6 PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA

Not Applicable. TunTrust does not support Certificate modification.

4.8.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Not Applicable. TunTrust does not support Certificate modification.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 CIRCUMSTANCES FOR REVOCATION

Certificate revocation is the process by which TunTrust prematurely terminates the Validity of a Certificate. TunTrust will make its certificate revocations public through the use of publicly issued CRLs and publicly available OCSP responder services.

4.9.1.1 REASONS FOR REVOKING A SUBSCRIBER CERTIFICATE

With the exception of Short-lived Subscriber Certificates, TunTrust revokes a Certificate within 24 hours and uses the corresponding CRLReason (see Section 7.2.2) if one or more of the following occurs:

1. The Subscriber requests in writing, without specifying a CRLreason, that TunTrust revoke the Certificate (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
2. The Subscriber notifies TunTrust that the original Certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);
3. TunTrust obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);
4. TunTrust is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate, including but not limited to those identified in 6.1.1.3 (CRLReason #1, keyCompromise);

TunTrust obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon (CRLReason #4, superseded).With the exception of Short-lived Subscriber Certificates,TunTrust revokes a Certificate within 5 days and uses the corresponding CRLReason (see Section 7.2.2) if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 (CRLReason #4, superseded);
2. TunTrust obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);
3. TunTrust is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement (CRLReason #9, privilegeWithdrawn);
4. TunTrust is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name (CRLReason #5, cessationOfOperation);
5. TunTrust is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn);
6. TunTrust is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);
7. TunTrust is made aware that the Certificate was not issued in accordance with the Baseline Requirements or the present CP/CPS (CRLReason #4, superseded);
8. TunTrust determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
9. TunTrust's right to issue Certificates under these Requirements expires or is revoked or terminated, unless TunTrust has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
10. Revocation is required by this CP/CPS for a reason that is not otherwise required to be specified by this section 4.9.1.1 (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL); or
11. TunTrust is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise).

4.9.1.2 Reasons for revoking a Subordinate CA Certificate

TunTrust does not have any third party Subordinate CAs. The only CAs that TunTrust operates are the ones listed in section 1.3.1.

TunTrust Issuing CAs will revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing;

2. The Subordinate CA notifies TunTrust Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;

3. TunTrust Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;

4. TunTrust Issuing CA obtains evidence that the Certificate was misused;

5. TunTrust Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with the CA/B Forum Baseline Requirements or the applicable CP/CPS;

6. TunTrust Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;

7. TunTrust Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;

8. TunTrust Issuing CA's or Subordinate CA's right to issue Certificates under the CA/B Forum Baseline Requirements expires or is revoked or terminated, unless TunTrust Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or

9. Revocation is required by TunTrust Issuing CA's Certificate Policy and/or Certification Practice Statement.

4.9.2 WHO CAN REQUEST REVOCATION

TunTrust accepts authenticated requests for revocation. Authorization for revocation shall be accepted if the revocation request is received from either the Subscriber or its appropriately authorized Certificate Manager.

Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports to notify TunTrust of a suspected reasonable cause to revoke the Certificate. Problem Reports shall be submitted to the Contact Person specified in Section 1.5.2. TunTrust may also at its own discretion revoke Certificates.

4.9.3 PROCEDURE FOR REVOCATION REQUEST

A revocation request should be promptly and directly communicated to TunTrust. A revocation request may be submitted using one of the following methods:

- Using TunTrust revocation online service available at https://www.tuntrust.tn/Revocation-online-service. In this case, the Subscriber is required to provide:
    - The FQDN listed in the certificate that needs to be revoked, and
    - An email address to confirm the Subscriber's control over the listed FQDN, as per section 3.2.2.4.2 and section 3.2.2.4.4 of the present CP/CPS. A revocation challenge will be sent to this email and the Subscriber needs to provide it for the certificate revocation to be processed.

- Physical presence before a TunTrust RA operator: Either the Certificate Manager or the Legal Representative of the Subscriber must be physically present at the headquarters (Section 1.5.2) of TunTrust and request the revocation of a Certificate in writing after providing a valid ID.

For Certificate Problem Report submitted by third parties to the Contact Person specified in Section 1.5.2, TunTrust personnel begins investigating the request within 24 hours after receipt and decide whether revocation is appropriate based on the following criteria:

- The nature of the alleged problem,
- The evidence provided in support of the request,
- The urgency of the request,
- The number of reports received about a particular certificate or website,
- The identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered),

- and Tunisian National Legislation.

4.9.4 REVOCATION REQUEST GRACE PERIOD

No grace period is permitted once a revocation request has been verified. TunTrust will revoke Certificates according to sections 4.9.1.

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

Within 24 hours after receiving a Certificate Problem Report, TunTrust will investigate the facts and circumstances related to the Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, TunTrust will work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which TunTrust will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation does not exceed the time frame set forth in Section 4.9.1.1.

4.9.6 REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES

Relying parties must validate every Certificate against the most updated CRL as minimum. Alternatively, relying parties may check Certificate status using OCSP.

4.9.7 CRL ISSUANCE FREQUENCY

CRLs are available via a publicly-accessible HTTP URL (i.e., “published”) as stated in Appendix A and B.

Within twenty-four (24) hours of issuing its first Certificate, TunTrust generates and publishes a full and complete CRL.

TunTrust CAs issuing Subscriber Certificates:

1. update and publish a new CRL at least every:
   - seven (7) days if all Certificates include an Authority Information Access extension with an id-ad-ocsp accessMethod (“AIA OCSP pointer”); or
   - four (4) days in all other cases;
2. update and publish a new CRL within twenty-four (24) hours after recording a Certificate as revoked.

TunTrust CAs issuing CA Certificates:

1. update and publish a new CRL at least every twelve (12) months;
2. update and publish a new CRL within twenty-four (24) hours after recording a Certificate as revoked.

TunTrust continues issuing CRLs until one of the following is true:

- all Subordinate CA Certificates containing the same Subject Public Key are expired or revoked; OR
- the corresponding Subordinate CA Private Key is destroyed.

4.9.8 MAXIMUM LATENCY FOR CRLS

The CRLs of TunTrust CA are issued according to section 4.9.7 and published in a timely manner. The revocation becomes effective immediately upon its publication.

4.9.9 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

The validity interval of an OCSP response is the difference in time between the `thisUpdate` and `nextUpdate` field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

A certificate serial is "assigned" if:

- a Certificate or Precertificate with that serial number has been issued by the Issuing CA; or

- a Precertificate with that serial number has been issued by a Precertificate Signing Certificate, as defined in Section 7.1.2.4, associated with the Issuing CA.

A certificate serial is "unassigned" if it is not "assigned".

The following applies for communicating the status of Certificates and Precertificates which include an Authority Information Access extension with an id-ad-ocsp accessMethod.

The OCSP responder operated by TunTrust supports the HTTP GET method as described in RFC 6960 and/or RFC 5019.

- For the status of Subscriber Certificate or its corresponding Precertificate :
  - TunTrust OCSP responses have a validity interval greater than or equal to eight hours;
  - TunTrust OCSP responses have a validity interval less than or equal to ten days;
  - TunTrust OCSP responses have validity intervals less than sixteen hours, therefore TunTrust updates the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.
- For the status of Issuing CA Certificates, TunTrust provides an updates OCSP response at least every twelve months; and within 24 hours after revoking the Certificate.

The following applies for communicating the status of all Certificates for which an OCSP responder is willing or required to respond.

TunTrust OCSP responses conform to RFC 6960 and/or RFC 5019. OCSP responses are signed by an OCSP Responder which complies with the OCSP Responder Certificate Profile in Section 7.1.2.8.

If the OCSP Responder receives a request for the status of a Certificate serial number that is "unassigned", then the responder does not respond with a "good" status.

4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS

TunTrust supports OCSP responses in addition to CRLs. Relying Parties must confirm revocation information otherwise all warranties become void.

4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

TunTrust does not employ any method other than OCSP and CRL for advertising revocation status.

4.9.12 SPECIAL REQUIREMENTS RELATED TO KEY COMPROMISE

Should a Private Key become compromised, the related Certificate shall immediately be revoked. Should the private CA key become compromised, all Certificates issued by that CA shall be revoked.

In order to demonstrate Key Compromise, Parties must submit Certificate problem reports to TunTrust (refer to section 1.5.2) that include one of the following methods:

- Submission of a signed CSR signed by the compromised Private Key and verifiable by the Public Key,
- Providing the Private Key itself,
- Providing references to vulnerability and/or security incident sources from which the Key Compromise is verifiable.

4.9.13 CIRCUMSTANCES FOR SUSPENSION

No suspension of Certificates is performed by TunTrust.

4.9.14 WHO CAN REQUEST SUSPENSION

No suspension of Certificates is performed by TunTrust.

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

No suspension of Certificates is performed by TunTrust.

4.9.16 LIMITS ON SUSPENSION PERIOD

No suspension of Certificates is performed by TunTrust.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 OPERATIONAL CHARACTERISTICS

TunTrust provides a Certificate status service either in the form of a CRL distribution point or an OCSP responder or both in the Certificates. TunTrust does not remove revocation entries on CRL or OCSP until after the Expiry Date of the revoked Certificate.

4.10.2 SERVICE AVAILABILITY

TunTrust operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of five seconds or less under normal operating conditions.

TunTrust maintains an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by TunTrust.

TunTrust maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3 OPTIONAL FEATURES

The OCSP Responder is available for all types of certificates issued by TunTrust.

4.11 End of Subscription

Subscribers may end their subscription to Certificate services by having their Certificate revoked or naturally letting it expire.

4.12 Key Escrow and recovery

The private keys for each CA Certificate were generated and are stored in Hardware Security Modules (HSM) and are backed up but not escrowed.

4.12.1 Key escrow and recovery Policy and practices

TunTrust CA key-recovery is based on HSM standard key-backup where the keys in the backup are protected with encryption mechanism. All HSM backups and administrator smartcards are stored in a safety vault. Only persons performing Trusted Roles have the access to the safety vault.

TunTrust does not store copies of Subscriber private keys; Subscriber's key back-up, escrow and key recovery are not possible.

4.12.2 Session key encapsulation and recovery policy and practices

TunTrust does not provide session key encapsulation and recovery.

5 Facility, Management, and operational controls

TunTrust develops, implements, and maintains a comprehensive information security policy designed to:

1. Protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;
2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;
3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;
4. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and
5. Comply with all other security requirements applicable to TunTrust by law.

The Certificate Management Process includes:

1. Physical security and environmental controls;
2. System integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
3. Network security and firewall management, including port restrictions and IP address filtering;
4. User management, separate trusted-role assignments, education, awareness, and training; and
5. Logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

TunTrust performs an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that TunTrust has in place to counter such threats.

Based on the Risk Assessment, TunTrust develops, implements, and maintains a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes.

The security plan also takes into account then-available technology and the cost of implementing the specific measures, and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.1 PHYSICAL CONTROLS

5.1.1 SITE LOCATION AND CONSTRUCTION

TunTrust CA's primary and secondary data centers are in Tunis, Tunisia. TunTrust data center exhibits the following features:

- Protected with physical barriers, including solid walls that extend from real floor to real ceiling to prevent unauthorized entry and environmental contamination to the CAs certificate manufacturing facility. Not located in areas likely to exhibit hazard of environmental damage, chemical, biological or radiological pollution,
- Physically separated areas for visitor reception, clearance and computer equipment hosting,
- Capable of safely storing, separate to any computer equipment, fuel to power facilities in the event of loss of mains power.

5.1.2 PHYSICAL ACCESS

Entry to TunTrust Data Centers containing the CAs certificate manufacturing facility is achieved only through a limited number of access points controlled by security personnel on duty full time (24 hours per day, 365 days per year).

Intruder detection systems including infrared walls are installed and regularly tested to cover all external doors of the data centers housing the CA operational facilities.

All critical CA operations take place within a physically secure facility with at least four layers of security to access sensitive hardware or software. Such systems are physically separated from the organization's other systems so that only authorized employees of the CA can access them.

The secure parts of TunTrust CA hosting facilities are protected using physical access controls with biometric scanners or card access systems making them accessible only to appropriately authorized individuals. CA operational facilities are physically locked and alarmed when unoccupied.

All personnel and visitors entering and leaving CA operational facilities are logged. Entry, exit, and activities within CA facilities are under constant video surveillance. Third party support services personnel are granted restricted access to secure CA operational facilities only when required and such access is authorized and accompanied. Access rights to CA facilities are regularly reviewed and updated.

5.1.3 POWER AND AIR CONDITIONING

TunTrust CA operates within data centers that have primary and secondary power supplies to ensure continuous, uninterrupted access to electric power. Redundant backup power is provided by battery uninterrupted power supplies (UPS) and one generator.

TunTrust data centers are equipped with heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4 WATER EXPOSURES

No data center is in a known flood risk area. All TunTrust CAs certificate manufacturing facility have sealed roofs to prevent water exposure.

HVAC systems are in place to prevent humidity buildup. All data centers have policies preventing the taking of liquids (e.g. drinks) into the cabinet areas.

5.1.5 FIRE PREVENTION AND PROTECTION

TunTrust has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke.

Fire doors exist on security perimeters around CA operational facilities and are alarmed.

TunTrust's fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6 MEDIA STORAGE

All media containing production software and data, audit, archive, or backup information are stored within TunTrust facilities with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage such as water, fire, and electromagnetic.

5.1.7 WASTE DISPOSAL

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance to the manufacturer s' guidance prior to disposal.

5.1.8 OFF-SITE BACKUP

TunTrust maintains copies of CA private keys, archived audit logs, and other sensitive information at secured off-site locations. All copies of private keys are stored in a system or device validated as meeting FIPS 140 Level 3 to ensure that they are only accessible by trusted personnel.

5.2 PROCEDURAL CONTROLS

5.2.1 TRUSTED ROLES

TunTrust personnel in Trusted Roles include, but are not limited to, CA and system administration personnel and personnel involved with customer support and vetting. An additional role to TunTrust is the Auditor role, performed by TunTrust's internal auditors.

The functions and duties performed by persons in Trusted Roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of TunTrust. All personnel appointed to a trusted role had a background check prior to allowing such person to act in a trusted role. A list of personnel appointed to Trusted Roles is maintained and reviewed at least annually.

The following roles are deemed to be Trusted Roles:

Validation Specialist	Employees responsible for routine certification services such as customer services, document control, processes relating to Subscriber Certificate registration, generation and revocation. They are also responsible for interacting with Applicants and Subscribers, managing the Certificate request queue and completing the Certificate approval checklist as identity vetting items are successfully completed. A person to whom this role is assigned can be a shareholder of CA private keys activation data.
System Administrator	The System Administrator is responsible for the installation and configuration of PKI components (CA, RA, ...). This administrator is also responsible for keeping PKI systems updated with software patches and other maintenance needed for system stability and recoverability. A person to whom this role is assigned can be a shareholder of CA private keys activation data.
System Operator	The System Operator is responsible for the installation and configuration of the system hardware, including servers and different components of the Front End / Internal Support System. The System Administrator is also responsible for keeping systems updated with software patches and other maintenance needed for system stability and recoverability. A person to whom this role is assigned can be a shareholder of CA private keys activation data.
Application Administrator	The Application Administrator is a trusted role. This administrator is responsible for the installation, configuration and operations of the applications related to TunTrust.
Physical and Logical Security Officer	The Physical and Logical Security Officer is a trusted role. This role is responsible for the installation and configuration of the physical security platforms (access control, video surveillance, IDS, ...) and the logical security platforms (firewalls, WAF, routers, network configuration). A person to whom this role is assigned can be a shareholder of CA private keys activation data.
Auditor	The Auditor is authorized to view archives and audit logs. The auditor is also responsible for overseeing internal compliance to determine if TunTrust is operating in accordance with this CP/CPS. This includes acting as internal auditor in TunTrust key ceremonies. A person to whom

	this role is assigned cannot be a shareholder of CA private keys activation data.
Key/Ceremony Manager	The Key/Ceremony Manager is responsible of conducting the key ceremonies.
Shareholders	Holders of secret shares needed to operate TunTrust CA private keys.

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

TunTrust Private Key is backed up, stored, and recovered only by personnel in Trusted Roles using, at least, dual control in a physically secured environment.

Physical and logical access controls exist for the key activation material in order to maintain multi-party and multi-factor control over the Hardware Security Modules containing CA Private Keys.

Shareholders use HSM Smartcard for authentication. The HSM itself enforces dual control based on the HSM smartcards for different functions. The number of needed HSM-smartcards (m) of the total number of produced HSM-smartcards (n) is:

(a) Key generation of Root CA = 3 of 6

(b) Signing key activation of Root CA = 3of 6

(c) Private key backup and restore of Root CA = 3 of 6

(d) Key generation of Issuing CA = 2 of 6

(e) Signing key activation of Issuing CA = 2 of 6

(f) Private key backup and restore of Issuing CA = 3 of 6

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

All personnel are required to authenticate themselves before they are allowed access to systems necessary to perform their Trusted Roles.

5.2.4 ROLES REQUIRING SEPARATION OF DUTIES

No person can have more than one of the roles listed in section 5.2.1 at a time.

To accomplish this separation of duties, TunTrust specifically designates individuals to Trusted Roles.

TunTrust's systems identify and authenticate individuals acting in Trusted Roles, restrict an individual from assuming multiple roles, and prevent any individual from having more than one identity.

5.3 PERSONNEL CONTROLS

5.3.1 QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS

TunTrust must abide by Tunisian public sector recruitment procedures based on open competition assessing the Qualifications, Experience, Clearance and Training of the candidates as appropriate to the job function.

Prior to the engagement of any TunTrust employee in the Certificate Management Process, , TunTrust verifies the identity and trustworthiness of such person who must be a TunTrust permanent employee. All TunTrust personnel must sign the internal security charter.

Trusted roles and responsibilities, as specified in Section 5.2.1 are documented in job descriptions. TunTrust personnel have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness.

5.3.2 BACKGROUND CHECK PROCEDURES

All TunTrust CA personnel are subject to Tunisian public sector recruitment and selection procedures prior to employment. These procedures undergo background checks, to the extend allowable by law, including, at a minimum:

- criminal records checks,
- employment and education history,
- identity checks using government issued photo ID.

TunTrust personnel do not have access to the trusted functions until all necessary checks are completed and results analyzed. All persons filling Trusted Roles are selected on the basis of loyalty, trustworthiness, and integrity, and are subject to background checks at least every five years.

5.3.3 TRAINING REQUIREMENTS

TunTrust provides suitable training to all staff before they take on a Trusted Role should they not already have the complete skill-set required for that role. Training of personnel is undertaken via a mentoring process involving senior members of the team to which they are attached.

TunTrust provides all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including this CP/CPS), common threats to the information verification process (including phishing and social engineering), and the CA/B Forum requirements. TunTrust maintains records of such training and ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.

TunTrust documents that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

TunTrust requires all Validation Specialists to pass an examination provided by TunTrust on the information verification requirements outlined in this CP/CPS.

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

All personnel in Trusted Role maintain skill levels consistent with TunTrust's training and performance programs.

Individuals responsible for Trusted Roles are aware of changes in TunTrust CA or RA operations, as applicable. Any significant change to the operations has a training plan, and the execution of such plan is documented.

TunTrust provides an information security and privacy training at least once a year to all employees.

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

Job rotation of employees is done as necessity arises, depending on the needs of TunTrust, or by request of an individual employee.

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

All employees of TunTrust are made aware that performing actions outside the rules established by operational regulation, security policy or privacy policy carries the possibility of disciplinary action as per TunTrust internal rules and Tunisian Public sector disciplinary procedures.

Should that violation of company policy encompass potential criminal wrongdoing, TunTrust will report the matter to the appropriate law enforcement bodies for further investigation and action as stated in the Tunisian Public sector disciplinary procedures.

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

TunTrust does not assign Trusted Roles to external Contractors.

All Contract arrangements between Contractors and TunTrust for the provision of temporary contract personnel allow TunTrust to take measures against contract staff that violate TunTrust security policies.

Protective measures may include (i) bonding requirements on contract personnel; (ii) indemnification for damages due to contract personnel willful harmful actions; and (iii) financial penalties.

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

Personnel are granted access to relevant training documents and governance documents as their intended roles dictate. Other technical, operational and administrative documents (e.g., administrator manuals, user manuals, etc.) are provided in order for the trusted personnel to perform their duties.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 TYPES OF EVENTS RECORDED

TunTrust records events related to the security of its Certificate System, Root CA Systems, and Delegated Third Party Systems. TunTrust records events related to their actions taken to process a Certificate request and to issue a Certificate, including all information generated and documentation received in connection with the Certificate request; the time and date; and the personnel involved. TunTrust makes these records available to its Qualified Auditor. TunTrust records at least the following events:

1. CA certificate and key lifecycle events, including:
    1. Key generation, backup, storage, recovery, archival, and destruction;
    2. Certificate requests, renewal, and re-key requests, and revocation;
    3. Approval and rejection of certificate requests;
    4. Cryptographic device lifecycle management events;
    5. Generation of Certificate Revocation Lists;
    6. Signing of OCSP Responses (as described in Section 4.9 and Section 4.10); and
    7. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. Subscriber Certificate lifecycle management events, including:
    1. Certificate renewal, and re-key requests, and revocation;
    2. All verification activities stipulated in the Baseline Requirements and this CP/CPS;
    Effective 2026-07-15, records MUST include at a minimum:

1. the information being validated (e.g., the applied-for FQDN or the organization name);
2. the ADN used (if applicable and different from the applied-for FQDN); and
3. the validation method used (e.g., the BRs section number or the registered label of an ACME validation method);

3. Approval and rejection of Certificate requests;
4. Issuance of Certificates;
5. Generation of Certificate Revocation Lists; and
6. Signing of OCSP Responses (as described in Section 4.9 and Section 4.10).
7. Multi-Perspective Issuance Corroboration attempts from each Network Perspective, minimally recording the following information:
    a. an identifier that uniquely identifies the Network Perspective used;
    b. the attempted domain name and/or IP address; and
    c. the result of the attempt (e.g., "domain validation pass/fail", "CAA permission/prohibition").
8. Multi-Perspective Issuance Corroboration quorum results for each attempted domain name or IP address represented in a Certificate request (i.e., "3/4" which should be interpreted as " Three (3) out of four (4) attempted Network Perspectives corroborated the determinations made by the Primary Network Perspective).

3. Security events, including:
    1. Successful and unsuccessful PKI system access attempts;
    2. PKI and security system actions performed;
    3. Security profile changes;
    4. Installation, update and removal of software on a Certificate System;
    5. System crashes, hardware failures, and other anomalies;
    6. Relevant router and firewall activities (as described in Section 5.4.1.1); and
    7. Entries to and exits from the CA facility.

Log records include the following elements:

- Date and time of event;
- the identity of the entity and/or operator that caused the record (when applicable); and
- Description of the event.

All TunTrust CA components are regularly synchronized with a reliable time service. TunTrust CA uses a GPS-NTP time source to establish the correct time for accurate recording of automated log events.

Private keys in any form (e.g., plaintext or enciphered) are never recorded in Audit Logs.

5.4.1.1 ROUTER AND FIREWALL ACTIVITIES LOGS

Logging of router and firewall activities necessary to meet the requirements of Section 5.4.1, Subsection 3.6 MUST at a minimum include:

1. Successful and unsuccessful login attempts to routers and firewalls; and
2. Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and
3. Logging of all changes made to firewall rules, including additions, modifications, and deletions; and
4. Logging of all system events and errors, including hardware failures, software crashes, and system restarts.

5.4.2 FREQUENCY OF PROCESSING LOG

The logging process allows real-time recording of transactions to identify abnormalities related to failed attempts (access or instruction). In case of manual input, writing is made the same business day as the event. Log events deemed to be security sensitive will automatically generate security incident reports that are handled as defined in section 5.7.

A human review of the logging processes is also performed on application and system logs at least once every 30 days to validate the integrity of logging processes and ensure that monitoring, logging, alerting, and log integrity-verification functions are operating properly.

5.4.3 RETENTION PERIOD FOR AUDIT LOG

TunTrust retains for at least 20 years as per Tunisia national law:

1. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1 (1)) after the later occurrence of:
    1. the destruction of the CA Private Key; or
    2. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the CA field set to TRUE and which share a common Public Key corresponding to the CA Private Key;
2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1(2)) after the expiration of the Subscriber Certificate;
3. Any security event records (as set forth in Section 5.4.1 (3)) after the event occurred.

TunTrust makes these audit logs available to its Qualified Auditor upon request.

5.4.4 PROTECTION OF AUDIT LOG

Audit logs are stored within TunTrust primary location and in an off-site location. Access and security controls are in place to prevent alteration with the audit log. Production and archived logical audit logs are protected using a combination of physical and logical access controls.

All automated log events are recorded real-time to a secured central logging services in order to prevent log shrinkage or unexpected alteration. Logs stored offsite reside in facilities which have protections at least equivalent to the TunTrust originating systems.

Off-site logs are digitally signed to make tampering of the logs evident. The encryption key used for signing audit logs is not used for any other purpose. Offsite logs are verified periodically to ensure that their integrity has been maintained.

5.4.5 AUDIT LOG BACKUP PROCEDURES

For CA components that allow the configuration of multiple logging end-points, automated log events are recorded real-time to central logging services located at TunTrust Primary datacenter and at the secondary data center as an off-site location.

For CA components that do not support multiple logging end-points, TunTrust makes backup copies of audit logs on a monthly basis according to internal backup procedures. These copies are kept in a safe protected using physical access controls.

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

Automated audit data is generated and recorded at the application, network and operating system level. All automated audit logs are sent to a central logging service for collation and review. Manually generated audit data is recorded by TunTrust personnel assigned to Trusted Roles.

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

TunTrust is not required to notify a subject that it has been the cause of an auditable event.

5.4.8 VULNERABILITY ASSESSMENTS

TunTrust undergoes a vulnerability scan (i) within one (1) week of receiving a request from the CA/Browser Forum, (ii) after any system or network changes that TunTrust determines are significant, and (iii) at least every three (3) months on public and private IP addresses identified as TunTrust's Certificate System.

TunTrust also undergoes a Penetration Test on Certificate Systems on at least an annual basis and after infrastructure or application upgrades that TunTrust determines are significant.

TunTrust records will be maintained in a manner reasonably sufficient to demonstrate that each Vulnerability Scan and Penetration Test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test.

TunTrust maintains and implements a formal documented vulnerability management process that includes identification, review, response, and remediation of vulnerabilities as described in Section 6.6.

Effective 15-Apr-2026, these policies and procedures MUST apply to Security Support Systems and Network Boundary Controls.

Additionally, TunTrust performs annual risk assessments that:

- Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Process;
- Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
- Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that TunTrust has in place to counter such threats.

5.5 RECORDS ARCHIVAL

5.5.1 TYPES OF RECORDS ARCHIVED

TunTrust archives all audit logs (as set forth in Section 5.4.1).

Additionally, TunTrust archives:

1. Documentation related to the security of its Certificate System, and Root CA System;
2. Documentation related to its verification, issuance, and revocation of certificate requests and Certificates.

TunTrust backs up application, network and system data including:

- Registration information of Subscribers (signed subscriber agreements, IDs of Subscribers, signed Certificate request Forms, proof of legal existence of the organization, etc.),
- Configuration files of TunTrust CA systems,
- All audit logs listed in section 5.4.1,
- Certificate lifecycle information,
- All versions of the CP/CPS and internal documents, including security policies and procedures,
- Ceremony scripts of TunTrust CA key events.

5.5.2 RETENTION PERIOD FOR ARCHIVE

Archived audit logs (as set forth in Section 5.5.1 are retained for a period of at least twenty (20) years from their record creation timestamp, or as long as they are required to be retained per Section 5.4.3, whichever is longer.

Additionally, TunTrust retains, for at least twenty (20) years:

1. All archived documentation related to the security of Certificate System, and Root CA System(as set forth in Section 5.5.1); and
2. All archived documentation relating to the verification, issuance, and revocation of certificate requests and Certificates (as set forth in Section 5.5.1) after the later occurrence of:
    1. such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates; or
    2. the expiration of the Subscriber Certificates relying upon such records and documentation.

5.5.3 PROTECTION OF ARCHIVE

Physical and logical access controls are in place to prevent unauthorized access to archived data in electronic form. Archives are retained and protected against modification or destruction. Only specific TunTrust Trusted Roles, and auditors may view the archives in whole. The contents of the archives will not be released as a whole, except as required by law.

5.5.4 ARCHIVE BACKUP PROCEDURES

TunTrust maintains and implements backup procedures so that in the event of the loss or destruction of the primary archives a complete set of backup copies is readily available.

5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

TunTrust ensures that the precise time of archiving all events, records and documents listed in section 5.4 and 5.5 is recorded. This is accomplished through accurate NTP synchronization of all systems with TunTrust NTP server. Records in paper format have a manually entered date and time.

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

Archive information is collected internally by TunTrust.

5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

TunTrust will not divulge archive information to any external party except as follows:

- Where a competent legal authority presents a warrant compelling the release of archived data; or
- Where an audit requires archived data in order to complete a compliance report ;
- Where archived data is electronically generated, the signatures and encryption of this data are checked to ensure its integrity was maintained.

5.6 KEY CHANGEOVER

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of the CA Private Key's lifetime, TunTrust ceases using its expiring CA Private Key to sign Certificates (two years prior to its expiration) and uses the old Private Key only to sign CRLs until the expiry of the last certificate issued under it.

A new CA signing key pair is commissioned and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA Certificate expiration. The corresponding new CA public key Certificate is provided to Subscribers and relying parties through the delivery methods detailed in Section 6.1.4.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

5.7.1.1 INCIDENT RESPONSE AND DISASTER RECOVERY PLANS

TunTrust has an Incident Response Procedure and a Disaster Recovery Plan. TunTrust documents a business continuity procedure and disaster recovery plan designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure.

TunTrust does not disclose business continuity plans to Subscribers, Relying Parties, or to Application Software Suppliers, but will provide business continuity procedure and the risk treatment plan to the TunTrust auditors upon request.

TunTrust annually tests, reviews, and updates these procedures. The business continuity procedure includes:

1. The conditions for activating the plan,
2. Emergency procedures,
3. Fallback procedures,
4. Resumption procedures,
5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective (RTO);

9. Regular testing of contingency plans;

10. TunTrust's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes ;

11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;

12. What constitutes an acceptable system outage and recovery time ;

13. How frequently backup copies of essential business information and software are taken;

14. The distance of recovery facilities to TunTrust main site; and

15. Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

When TunTrust CA fails to comply with any requirement of this CP/CPS - whether it be a misissuance, a procedural or operational issue, or any other variety of non-compliance - the event is classified as an incident. At a minimum, TunTrust will promptly report all incidents to Mozilla in the form of an Incident Report, and will regularly update the Incident Report until the corresponding bug is marked as resolved in the mozilla.org Bugzilla system by a Mozilla representative. TunTrust CA will cease issuance until the problem has been prevented from reoccurring.

5.7.1.2 MASS REVOCATION PLANS

As of 2025-09-01, TunTrust has a mass revocation plan, it maintains a comprehensive and actionable plan for mass revocation events, it performs annual testing of the mass revocation plan, and it incorporates lessons learned into such plan in order to continually improve its preparedness for mass revocation events over time.

TunTrust's mass revocation plan includes clearly defined, actionable, and comprehensive procedures designed to ensure rapid, consistent, and reliable response to large-scale certificate revocation scenarios. TunTrust is not required to publicly disclose its mass revocation plan or procedures but it makes them available to its auditors upon request. TunTrust annually tests, reviews, and updates its plan and such procedures.

Mass revocation provisions include:

1. Activation criteria – specific, objective, and measurable thresholds at which the mass revocation plan is triggered based on the CA's risk profile, issuance volumes, and operational capabilities;
2. Customer contact information – how subscriber and customer contact details are stored, maintained, and kept up to date;
3. Automation points – processes that are automated or could be automated, and those processes that require manual intervention;
4. Targets and timelines – for incident triage, revocation initiation, certificate replacement, and post-event review;
5. Subscriber notification methods – mechanisms for notifying impacted Subscribers;
6. Role assignments – roles and responsibilities of personnel responsible for initiating, coordinating, and executing the plan;
7. Training and education – training, awareness, and readiness activities for personnel responsible for, or supporting, the plan;
8. Plan testing – annual operational testing to assess readiness and demonstrate implementation feasibility, using one or more of tabletop exercises, simulations, parallel testing, or controlled test environments that DO NOT involve the revocation of active Subscriber Certificates; and

9. Post-test analysis and update schedule – how lessons learned from testing or live incidents are incorporated into the plan, and how often it is reviewed and updated.

5.7.2 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

TunTrust CA hosts—including Issuing CA, Certificate System, Security Support System, and Front-End / Internal-Support Systems- are built and maintained by a consistent configuration management process. Configuration changes to these systems are automatically captured and sent to a central monitoring service to determine whether any changes violated the CA's security policies.

If TunTrust determines that such systems have been compromised, TunTrust will investigate the extent of the compromise and the risk presented to affected parties. Depending on the extent of the compromise and after ensuring the integrity of the CA systems, TunTrust will re-initiate its operations on replacement hardware located at the off-site facility, using back-up copies of its software, data, and Private Keys. TunTrust reserves the right to revoke affected Certificates and to provide new public keys to users.

5.7.3 ENTITY PRIVATE KEY COMPROMISE PROCEDURES

In the event that a TunTrust CA private key has been or is suspected to have been compromised, TunTrust personnel will immediately convene an emergency Incident Response Team to assess the situation and to determine the degree and scope of the incident and take appropriate action. The following actions outline as follows:

- Collect all information related to the incident (and if the event is ongoing, ensure that all data are being captured and recorded);
- Begin investigating the incident and determine the degree and scope;
- The Incident Response Team determines the course of action or strategy that should be taken (and in the case of Private Key compromise, determining the scope of Certificates that must be revoked);
- Contact law enforcement, and other interested parties and activate any other appropriate additional security measures;
- Monitor system, continue the investigation, ensure that all data is still being recorded as evidence and make a forensic copy of data collected;
- Isolate, contain and stabilize the system, applying any possible short-term fixes needed to return the system to a normal operating state;
- Prepare an incident report that analyzes the cause of the incident and implement long-term solutions.

A new CA Key Pair should be generated and a new CA Certificate should be signed in accordance with the procedures outlined in Section 6 (Technical Security Controls) of this CP/CPS.

TunTrust will also notify Mozilla and other root stores in the event of a key compromise.

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

TunTrust Disaster Recovery Plan is tested, verified and updated at least annually to be operational in the event of a disaster.

TunTrust systems are redundantly configured at its primary facility and are mirrored at a separate geographically location for failover in the event of a disaster. TunTrust keeps activation data of the HSM of the disaster recovery site at a second separate geographically location.

If a disaster causes TunTrust PKI operations to become inoperative at the primary site, TunTrust will re-initiate its operations at its disaster recovery site, following the Disaster Recovery Plan and Business Continuity Procedure in order to recover TunTrust CA operations, giving priority to the ability to generate Certificate status information and thereafter certificate revocation and issuance.

5.7.5 MISS-ISSUANCE HANDLING PROCEDURES

In miss-issuance cases, TunTrust will immediately cease issuance from the affected part of TunTrust PKI until the source of the problem has been diagnosed and identified.

Once the problem is diagnosed, TunTrust will put in place at minimum temporary or manual procedures to prevent the problem from re-occurring until a fully automated fix is applied in a reasonable amount of time. TunTrust will restart Certificate issuance after approval of the TunTrust Certificate Policy Authority.

As per Section 4.9.1.1, TunTrust will scan corpus of issued certificates and revoke all certificates found with the same issue.

TunTrust will report the miss-issuance incident to its auditor and to the browser root certificate programs of which TunTrust is a member at the earliest possible date post-incident. The incident report should cover at least the following topics:

- How TunTrust CA first became aware of the problem (e.g. via a problem report submitted to TunTrust, a notification from the browser root certificate programs of which TunTrust is a member, or internal self-audit), and the time and date.
- A timeline of the actions TunTrust CA took in response. A timeline is a date-and-time-stamped sequence of all relevant events. This may include events before the incident was reported, such as when a particular requirement became applicable, or a document changed, or a bug was introduced, or an audit was done.
- The date and time TunTrust has stopped issuing certificates with the problem.
- A summary of the problematic Certificates. For each problem: number of Certificates, and the date the first and last Certificates with that problem were issued.
- The complete certificate data for the problematic certificates.
- Explanation about how and why the mistakes were made or bugs introduced, and how they avoided detection until now.
- List of steps TunTrust CA is taking to resolve the situation and ensure such issuance will not be repeated in the future, accompanied with a timeline of when TunTrust CA expects to accomplish these things and restart Certificate issuance.

5.8 CA OR RA TERMINATION

In case of termination of CA operations for any reason whatsoever, TunTrust will take the following steps prior to the termination:

- Provide subscribers of valid certificates, the operators of the browser root certificate programs and the CA/B Forum with ninety (90) days notice of its intention to cease acting as a CA,

- Revoke all certificates that are still un-revoked or un-expired at the end of the ninety (90) day notice period without seeking subscriber's consent,
- Destroy all private keys,
- Give timely notice of revocation to each affected Subscriber.

If a successor CA is found which can adopt all of TunTrust CA's responsibilities under its governing documentation, notification to the above shall also be provided explaining this succession. In such a case, the mass revocation may not be warranted.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

6.1.1.1 CA KEY PAIR GENERATION

For the Root CA Key Pairs, TunTrust performs the following controls:

1. prepares and follows a Key Generation Script,
2. has a Qualified Auditor witness the CA Key Pair generation process or records a video of the entire CA Key Pair generation process, and
3. has a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

In all cases, TunTrust performs the following controls:

1. generates the CA key Pair in a physically secured environment as described in section 5.1 of this CP/CPS;
2. generates the CA Key Pair using personnel in Trusted Roles under the principles of multiple person control and split knowledge as disclosed in section 6.2.1 of this CP/CPS;
3. generates the CA Key Pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in section 6.2.2 of this CP/CPS;
4. logs its CA Key Pair generation activities and logs all physical access during the key ceremony as disclosed in section 5.4 ; and
5. maintains effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in Section 6.2 of this CP/CPS and its Key Generation Script.

6.1.1.2 RA KEY PAIR GENERATION

No key pair generation is made for TunTrust RA.

6.1.1.3 SUBSCRIBER KEY PAIR GENERATION

TunTrust does not generate a Key Pair on behalf of a Subscriber and does not accept a certificate request using a Key Pair previously generated by TunTrust.

TunTrust rejects a Certificate request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in Sections 6.1.5 and/or 6.1.6

2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. TunTrust is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
4. TunTrust has previously been notified that the Applicant's Private Key has suffered a Key Compromise using TunTrust's procedure for revocation request as described in Section 4.9.3 and Section 4.9.12;
5. The Public Key corresponds to an industry-demonstrated weak Private Key. For requests submitted on or after November 15, 2024, at least the following precautions are to be implemented:
    1. In the case of Debian weak keys vulnerability (http://wiki.debian.org/SSLkeys), TunTrust rejects all keys found at https://github.com/cabforum/Debian-weak-keys/ for each key type (e.g. RSA, ECDSA) and size listed in the repository. For all other keys meeting the requirements of 6.1.5, with the exception of RSA key sizes greater than 8192 bits, TunTrust rejects Debian weak keys. see).
    2. In the case of ROCA vulnerability, TunTrust rejects keys identified by the tools available at https://github.com/crocs-muni/roca or equivalent.
    3. In the case of Close Primes vulnerability (https://fermatattack.secvuln.info/), TunTrust rejects weak keys which can be factored within 100 rounds using Fermat's factorization method.

    Suggested tools for checking for weak keys can be found here: https://cabforum.org/resources/tools/.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

Applicants are solely responsible for the generation of the private keys used in their Certificate Requests. TunTrust does not provide SSL key generation, escrow, recovery or backup operations.

If TunTrust becomes aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then TunTrust revokes all certificates that include the Public Key corresponding to the communicated Private Key.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

Subscribers generate Key Pairs and submit the Public Key to TunTrust in a CSR as part of the Certificate request process. The Subscriber's signature on the request is authenticated prior to issuing the Certificate.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

TunTrust publishes all CA certificates on its online repository https://www.tuntrust.tn/repository.

The browser root certificate programs of which TunTrust is a member will also embed Root Certificate Public Keys into root stores and operating systems.

6.1.5 KEY SIZES

TunTrust uses RSA key pairs and it:

- Ensures that the modulus size, when encoded, is at least 2048 bits, and;
- Ensure that the modulus size, in bits, is evenly divisible by 8.

TunTrust Certificates meet the following requirements for algorithm type and key size:

6.1.5.1 ROOT CA CERTIFICATES

	Value
Digest algorithm	SHA-256
RSA modulus size (bits)	4096

6.1.5.2 SUBORDINATE CA CERTIFICATES

	Value
Digest algorithm	SHA-256
RSA modulus size (bits)	4096

6.1.5.3 SUBSCRIBER CERTIFICATES

	Value
Digest algorithm	SHA-256
RSA modulus size (bits)	2048

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

TunTrust uses a HSM device that conforms to FIPS 186-4 and provides random number generation and onboard generation of up to 4096 bit RSA Public Key. The value of the public exponent is equal to : 65537.

TunTrust uses CA software that performs quality checks on generated keys for RSA algorithm and also performs regular internal audits against randomly selected samples of Subscriber Certificates per section 8.7.

6.1.7 KEY USAGE PURPOSES (AS PER X.509 V3 KEY USAGE FIELD)

Private Keys corresponding to Root Certificates are not used to sign Certificates except in the following cases:

- Self-signed Certificates to represent the Root CA itself;
- Certificates for Subordinate CAs and Cross-Certified Subordinate CA Certificates; and
- Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates).

The key usage extension is set in accordance with the certificate profile requirements specified in section 7.1.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

TunTrust implements physical and logical safeguards to prevent unauthorized Certificate issuance. Protection of the CA Private Key outside the validated system or device specified in section 6.2.7 consists of physical security and encryption, implemented in a manner that prevents disclosure of the CA Private Key. TunTrust encrypts its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

For subscriber keys, TunTrust requires that the private key holder uses reasonable steps to protect the key, such as restrictive permissions and possibly key encryption using a strong passphrase.

6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

The following list shows the requirements for the different users of hardware cryptographic modules are implemented:

- Root CA keys : The HSM used for CA keys meets FIPS 140-2 level 3 requirements;
- Issuing CAs keys: The HSM used for CA keys meets FIPS 140-2 level 3 requirements;
- Subscriber keys (SSL Certificate) : The Subscriber is fully responsible for his/her private keys.

A check of the integrity and tests of functionalities of HSMs are done by personnel in Trusted Roles upon delivery of the HSMs to TunTrust facility. In addition to that, TunTrust maintains controls to provide reasonable assurance that physical access to the HSMs is limited to authorized personnel in Trusted Roles.

6.2.2 PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL

In all instances, CA private keys are generated in a physically secure environment within cryptographic modules that are validated to FIPS 140-2 Level-3. CA Certificate signing keys are only used within this secure environment. Access to the modules within the TunTrust environment, including the private keys, is restricted by the use of token/smart cards and associated pass phrases. These smartcards and pass phrases are allocated among multiple Shareholders in Trusted Roles. Such allocation ensures that no one member of TunTrust personnel in Trusted Roles holds total control over any component of the system. The hardware security modules are always stored in a physically secure environment and are subject to security controls throughout their lifecycle.

The following list shows how multi-person controls are implemented:

- Root CA keys : Root CA keys can only be accessed on the physical and on the logical level by adhering to '3 out of 6' control, meaning that 3 of the 6 persons are present.
- Issuing CAs keys : Management access to these keys is only possible using '4-eye' principle (2 out of 6).
- Subscriber keys: The Subscriber has single-person control of the Subscriber keys.

6.2.3 PRIVATE KEY ESCROW

TunTrust does not escrow Private Keys for any reason.

6.2.4 PRIVATE KEY BACKUP

TunTrust creates backup copies of CA private keys for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices under the same multi-person control as the original Private Key. Cryptographic modules used for private key

storage meet the requirements of this CP/CPS. Private keys are copied to backup hardware cryptographic modules in accordance with this CP/CPS.

6.2.5 PRIVATE KEY ARCHIVAL

TunTrust does not archive Subscriber Private Keys.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

TunTrust CA Private Keys are generated, activated and stored in Hardware Security Modules. Private Keys are exported from the HSM only for backup purposes. Private keys are transferred between HSMs according to manufacturers' specifications, and only leave the originating device in encrypted form.

When transported between cryptographic modules, the CA encrypts the private key and protects the keys used for encryption from disclosure.

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

TunTrust stores the CAs Private Keys on a FIPS 140-2 level 3 Hardware Security module which includes requirements to protect the Private Key and other assets against known threats.

6.2.8 METHOD OF ACTIVATING PRIVATE KEY

TunTrust is responsible for activating the Private Key in accordance with the instructions and documentation provided by the manufacturer of the hardware security module.

The following list shows how private keys are activated:

- Root CA keys: The Root CA keys are activated with three user keys (physical) and three user PINs (knowledge) ;
- Issuing CA keys: The Issuing CA keys are activated with two user keys (physical) and two user PINs (knowledge) ;
- Subscriber keys: Subscribers are solely responsible for protecting Private Keys in accordance with the obligations that are presented in Subscriber Agreement.

6.2.9 METHOD OF DEACTIVATING PRIVATE KEY

TunTrust deactivates access to its CA Private Keys and stores its cryptographic modules in a secure safe when not in use. TunTrust never leaves its HSM devices in an active unlocked or unattended state.

The method specified in Section 6.2.8 is operated for re-activation of private key.

6.2.10 METHOD OF DESTROYING PRIVATE KEY

TunTrust Private Keys are destroyed when they are no longer needed or when the Certificates to which they correspond have expired or have been revoked. Destroying Private Keys means that:

- TunTrust destroys all associated CA secret activation data in such a manner that no information can be used to deduce any part of the Private Key.
- TunTrust initializes the Hardware Security Module according to the specifications of the hardware manufacturer. In cases when this initialization procedure fails, TunTrust will physically destroy the device to remove the ability to extract any private key.

TunTrust does not generate private keys for Subscriber Certificates.

6.2.11 CRYPTOGRAPHIC MODULE RATING

See section 6.2.1.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVAL

Public keys, in the form of certificates and certificate requests are archived as per Section 5.5.

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

The Validity Periods of Certificates issued by TunTrust are as follows:

- The TunTrust Root CA is valid for 25 years from April 26th, 2019 to April 26th, 2044.
- The Validity Periods of the issuing CAs Certificates are 20 years from April 26th, 2019 to April 26th, 2039.
- Subscriber Certificates issued before 2026-03-15 SHOULD NOT have a Validity Period greater than 397 days and MUST NOT have a Validity Period greater than 398 days.
- Subscriber Certificates issued on or after 2026-03-15 and before 2027-03-15 SHOULD NOT have a Validity Period greater than 199 days and MUST NOT have a Validity Period greater than 200 days.
- Subscriber Certificates issued on or after 2027-03-15 and before 2029-03-15 SHOULD NOT have a Validity Period greater than 99 days and MUST NOT have a Validity Period greater than 100 days.
- Subscriber Certificates issued on or after 2029-03-15 SHOULD NOT have a Validity Period greater than 46 days and MUST NOT have a Validity Period greater than 47 days.

Certificate issued on or after	Certificate issued before	Maximum Validity Period
	2026-03-15	398 days
2026-**03-15**	2027-03-15	200 days
2027-**03-15**	2029-03-15	100 days
2029-**03-15**		47 days

TABLE 2: REFERENCE FOR MAXIMUM VALIDITY PERIODS OF SUBSCRIBER CERTIFICATES

For the purpose of calculations, a day is measured as 86,400 seconds. Any amount of time greater than this, including fractional seconds and/or leap seconds, shall represent an additional day.

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

TunTrust activates the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer. Generation and use of CA activation data used to activate CA Private Keys are made during a key ceremony. Activation data is assigned to shareholders in Trusted Roles as specified in section 5.2.1. The cryptographic hardware is held under multiple person control as explained in Section 5.2.2.

6.4.2 ACTIVATION DATA PROTECTION

TunTrust CA activation data is protected from disclosure through a combination of cryptographic and physical access control mechanisms. TunTrust Activation data is protected via FIPS 140-2 Level 3 devices and may only be used via registered data entry devices.

Repeated attempts to wrongly enter PIN data will cause the activation devices to lock out, and new device issuance to be required.

Subscribers are solely responsible for protecting their private keys activation credentials (PIN, password) and not share them with anyone else.

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

TunTrust CA activation data are only held by TunTrust personnel in Trusted Roles as specified in section 5.2.1.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

TunTrust uses a layered security approach to ensure the security and integrity of the computers used to run the CA software. The following non-exhaustive controls ensure the security of TunTrust operated computer systems:

- Strong identification and authentication for all accounts capable of directly causing Certificate Issuance (physical access control to enter in the room by ID badge and PIN + logic control by certificate to access the system);
- User rights management (to implement the access control policy defined by TunTrust CA, to implement the Principles of Least Privilege, multiple controls and separation of roles);
- Protection against computer viruses and other forms of compromise or unauthorized software and software updates from a trusted software repository;
- Security patches are applied within six (6) months of the security patch's availability, unless TunTrust documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch;
- Manage user accounts, including changes and the rapid removal of access rights;
- Network protection against intrusion of an unauthorized person using the firewall;
- Systems are segmented into networks based on their functional, or logical relationship;
- Networks are configured with rules that support only the services, protocols, ports, and communications that the CA has identified as necessary to its operations
- Secure and encrypted communication between systems;
- Monitoring and audit procedures of the system configuration, including routing elements, are in place.

6.5.2 COMPUTER SECURITY RATING

TunTrust has established a security framework which covers and governs the technical aspects of its computer security.

As described in section 5.4.8, the systems themselves and the services running on the systems are subject to thorough reviews and testing (including penetration testing). TunTrust operates also a vulnerability management process which includes monitoring of supplier security alerts.

The technical aspects of computer security are subject to periodic audits.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 SYSTEM DEVELOPMENT CONTROLS

TunTrust has mechanisms in place to control and monitor the acquisition and development of its CA systems.

Change requests require the approval of the change manager. Significant changes require the approval of TunTrust Board of Directors. All changes made to the CA systems are logged and tested before deployment.

In this manner, TunTrust can verify whether a change to the system has been properly evaluated for risk mitigation and authorized by management.

All acquisitions made by TunTrust follow the Tunisian national law for governmental procurements. This includes the publication of request for proposals and evaluating each proposal (thus each vendor) according to the set specifications.

All hardware and software are shipped under standard conditions with controls in place to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering. Quality assurance is maintained throughout the process through testing and documentation or by purchasing from trusted vendors. Updates of equipment or software are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel.

Since TunTrust uses Linting software developed by third parties, it monitors for updated versions of that software and endeavors to plan for updates no later than three (3) months from the release of the update.

TunTrust MAY perform Linting on the corpus of its unexpired, un-revoked Subscriber Certificates whenever it updates the Linting software.

6.6.2 SECURITY MANAGEMENT CONTROLS

TunTrust CAs establish formal mechanisms to document, control, monitor, and maintain the security-related configurations and the integrity software, firmware and hardware of its CA systems, including any modifications or upgrades. The TunTrust CA's monitoring control processes includes issuance of alerts automatically and in real time when any changes are detected.

6.6.3 LIFE CYCLE SECURITY CONTROLS

TunTrust applies recommended security patches to Certificate Systems within six months of the security patch's availability, unless it documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.

TunTrust does one of the following within 96 hours of discovery of a Critical Vulnerability not previously addressed by TunTrust CA's vulnerability correction process:

- Remediate the Critical Vulnerability;
- If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to (1) vulnerabilities with high CVSS scores, starting with the vulnerabilities TunTrust determines are the most critical (such as those with a CVSS score of 10.0) and (2) systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; or
- Document the factual basis for the TunTrust determination that the vulnerability does not require remediation because (a) TunTrust disagrees with the NVD rating, (b) the identification is a false positive, (c) the exploit of the vulnerability is prevented by compensating controls or an absence of threats; or (d) other similar reasons.

6.7 NETWORK SECURITY CONTROLS

TunTrust CA system is connected to one internal network and is protected by firewalls, a Demilitarized Zone (DMZ) and Network Address Translation for all internal IP addresses. TunTrust's customer support and vetting workstations are also protected by firewall(s) and only use internal IP addresses.

TunTrust maintains the Root CA Systems in a High Security Zone and in an offline state or air-gapped from all other networks. TunTrust Root CA Keys are kept offline and brought on-line only when necessary to sign Certificate Issuing CAs or periodic CRLs or OCSP Certificates. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems. It is TunTrust 's security policy to block all ports and protocols and open only necessary ports to enable CA functions.

All CA equipment is configured with a minimum number of services and accounts and all unused network ports, accounts and services are disabled. All firewall configurations and changes thereto are documented, authorized and implemented in accordance with change management procedures. Changes to network configuration policy go through the same change management process as host devices, and are similarly documented, reviewed and approved.

TunTrust CA network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement.

TunTrust implements automated mechanisms under the control of TunTrust Trusted Roles to process logged system activity and alert multiple destinations of possible Critical Security Events. TunTrust requires trusted role personnel to follow up on alerts of possible Critical Security Events.

TunTrust complies with the current version of the CA/Browser Forum's Network and Certificate System Security Requirements which are incorporated by reference as if fully set forth herein.

Effective September 8th 2025, the timeframes established for responding to and remediating vulnerabilities identified in Certificate Systems are as follows:

Criticality of the vulnerability	Timeframe set to respond to the vulnerability	Timeframe set to remediate the vulnerability
Critical	96 hours	30 days

High	5 days	45 days
Medium	15 days	3 months
Low	15 days	6 months

6.7.1 NETWORK SEGMENTATION

TunTrust's Infrastructure MUST are segmented into separate networks based on the functional and/or logical relationships of CA Infrastructure components.

Network segmentation SHOULD be designed and implemented in a manner that:

1. minimizes attack surfaces;
2. limits lateral movement within networks;
3. restricts traffic flow between different network segments; and
4. protects all CA Infrastructure components from unauthorized access.

Network segmentation MUST be designed and implemented using Network Boundary Controls, such as:

- firewalls
- networkswitches
- physically separate networks
- software-defined networking

Network segmentation MAY leverage software, such as:

- virtual local area networks (VLANs) and VLAN access control lists
- virtual private networks (VPNs)

6.7.2 CA INFRASTRUCTURE SECURITY

TunTrust's Infrastructure is in a Physically Secure Environment.

Root CASystems MUST be on physically separate networks from all other CA Infrastructure.

Connections to the TunTrust's Infrastructure are authenticated and encrypted, except where a formal specification(s) prohibits or limits the use of authentication and/or encryption. Connections within the CA Infrastructure or Network Boundary Controls SHOULD be authenticated and encrypted. CA Infrastructure and Network Boundary Controls are implemented and configured in a manner that minimizes unnecessary active components and capabilities such that:

1. all connections, communications, applications, services, protocols, and ports not used are removed and/or disabled; and

2. only connections, communications, applications, services, protocols, and ports necessary and approved under the Principle of Least Privilege are enabled.

Equivalent security MUST be implemented on all Systems on the same network as any CA Infrastructure component

6.8 TIME-STAMPING

All TunTrust CA components are regularly synchronized with a reliable time service. TunTrust CA uses a GPS-NTP time source to establish the correct time for:

- Initial validity time of a CA Certificate;
- Revocation of a CA Certificate;
- Posting of CRL updates; and
- Issuance of Subscriber end entity Certificates.

7 CERTIFICATE, CRL, AND OCSP PROFILES

Certificate issued under this CP/CPS conform to the RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

7.1 CERTIFICATE PROFILE

TunTrust meets the technical requirements set forth in Section 6.1.5 - Key Sizes, and Section 6.1.6

- Public Key Parameters Generation and Quality Checking.

The profiles of TunTrust CAs certificates are described in Appendix A of this CP/CPS.

The profiles of Subscribers certificates are described in Appendix B of this CP/CPS.

TunTrust issues Certificates in accordance with the profiles specified in theseRequirements.

7.1.1 VERSION NUMBER(S)

TunTrust CAs issue X.509 version 3 Certificates.

7.1.2 CERTIFICATE EXTENSIONS

All Certificates that TunTrust issues comply with one of the following certificate profiles described in section 7.1.2 of the Baseline Requirements, which incorporate, and are derived from RFC 5280. Except as explicitly noted, all normative requirements imposed by RFC 5280 shall apply, in addition to the normative requirements imposed by the Baseline Requirements.

X.509 v3 extensions are supported and used for Certificates profiles as described in Appendix A and Appendix B.

7.1.2.1 ROOT CA CERTIFICATE PROFILE

Field	Description
tbsCertificate	
version	MUST be v3(2)
serialNumber	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature	See Section 7.1.3.2

Field	Description
issuer	Encoded value MUST be byte-for-byte identical to the encoded subject
validity	See Section 7.1.2.1.1
subject	See Section 7.1.2.10.2
subjectPublicKeyInfo	See Section 7.1.3.1
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present
extensions	See Section 7.1.2.1.2
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

Appendix A of this CP/CPS describes TunTrust Root CA Certificate profile.

7.1.2.1.1 Root CA Validity

Field	Minimum	Maximum
notBefore	One day prior to the time of signing	The time of signing
notAfter	2922 days (approx. 8 years)	9132 days (approx. 25 years)

Note: This restriction applies even in the event of generating a new Root CA Certificate for an existing subject and subjectPublicKeyInfo (e.g. reissuance). The new CA Certificate MUST conform to these rules.

7.1.2.1.2 Root CA Extensions

Extension	Presence	Critical	Description
authorityKeyIdentifier	RECOMMENDED	N	See Section 7.1.2.1.3
basicConstraints	MUST	Y	See Section 7.1.2.1.4
keyUsage	MUST	Y	See Section 7.1.2.10.7
subjectKeyIdentifier	MUST	N	See Section 7.1.2.11.4
extKeyUsage	MUST NOT	-	-
certificatePolicies	NOT RECOMMENDED	N	See Section 0
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

7.1.2.1.3 Root CA Authority Key Identifier

Field	Description
keyIdentifier	MUST be present. MUST be identical to the subjectKeyIdentifier field.
authorityCertIssuer	MUST NOT be present
authorityCertSerialNumber	MUST NOT be present

7.1.2.1.4 Root CA Basic Constraints

Field	Description
cA	MUST be set TRUE
pathLenConstraint	NOT RECOMMENDED

7.1.2.2 Cross-Certified Subordinate CA Certificate Profile

Not Applicable. TunTrust does not have Cross-Certified Subordinate CAs.

7.1.2.3 Technically Constrained Non-TLS Subordinate CA Certificate Profile

Not Applicable. TunTrust does not have a technically constrained non-TLS Subordinate CA in this CA hierarchy.

7.1.2.4 Technically Constrained Precertificate Signing CA Certificate Profile

Not Applicable. TunTrust does not have a technically constrained precertificate signing CA.

7.1.2.5 Technically Constrained TLS Subordinate CA Certificate Profile

This Certificate Profile MAY be used when issuing TunTrust Certificate that will be considered Technically Constrained, and which will be used to issue TLS certificates directly or transitively.

Field	Description
tbsCertificate	
version	MUST be v3(2)
serialNumber	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature	See Section 7.1.3.2
issuer	MUST be byte-for-byte identical to the subject field of the Issuing CA. See Section 7.1.4.1
validity	See Section 7.1.2.10.1
subject	See Section 7.1.2.10.2
subjectPublicKeyInfo	See Section 7.1.3.1
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present
extensions	See Section 7.1.2.5.1
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.5.1 Technically Constrained TLS Subordinate CA Extensions

Extension	Presence	Critical	Description
authorityKeyIdentifier	MUST	N	See Section 7.1.2.11.1

basicConstraints	MUST	Y	See Section 7.1.2.10.4
certificatePolicies	MUST	N	See Section 0
crlDistributionPoints	MUST	N	See Section 7.1.2.11.2
keyUsage	MUST	Y	See Section 7.1.2.10.7
subjectKeyIdentifier	MUST	N	See Section 7.1.2.11.4
extKeyUsage	MUST[2]	N	See Section 7.1.2.10.6
nameConstraints	MUST	*[3]	See Section 7.1.2.5.2
authorityInformationAccess	SHOULD	N	See Section 7.1.2.10.3
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

7.1.2.5.2 TECHNICALLY CONSTRAINED TLS SUBORDINATE CA NAME CONSTRAINTS

For a TLS Subordinate CA to be Technically Constrained, Name Constraints extension MUST be encoded as follows. As an explicit exception from RFC 5280, this extension SHOULD be marked critical, but MAY be marked non-critical if compatibility with certain legacy applications that do not support Name Constraints is necessary.

nameConstraints requirements

Field	Description
permittedSubtrees	The permittedSubtrees MUST contain at least one GeneralSubtree for both of the dNSName and iPAddress GeneralName name types, UNLESS the specified GeneralName name type appears within the excludedSubtrees to exclude all names of that name type. Additionally, the permittedSubtrees MUST contain at least one GeneralSubtree of the directoryName GeneralName name type.
GeneralSubtree	The requirements for a GeneralSubtree that appears within a permittedSubtrees.
base	See following table.
minimum	MUST NOT be present.
maximum	MUST NOT be present.
excludedSubtrees	The excludedSubtrees MUST contain at least one GeneralSubtree for each of the dNSName and iPAddress GeneralName name types, unless there is an instance present of that name type in the permittedSubtrees. The directoryName name type is NOT RECOMMENDED.
GeneralSubtree	The requirements for a GeneralSubtree that appears within a permittedSubtrees.
base	See following table.

[2] While RFC 5280, Section 4.2.1.12 notes that this extension will generally only appear within end-entity certificates, the Baseline Requirements make use of this extension to further protect relying parties by limiting the scope of CA Certificates, as implemented by a number of Application Software Suppliers.

[3] See Section 7.1.2.10.8 for further requirements, including regarding criticality of this extension.

minimum	MUST NOT be present.
maximum	MUST NOT be present.

The following table contains the requirements for the GeneralName that appears within the base of a GeneralSubtree in either the permittedSubtrees or excludedSubtrees.

GeneralName requirements for the base field

Name Type	Presence	Permitted Subtrees	Excluded Subtrees	Entire Namespace Exclusion
dNSName	MUST	The CA MUST confirm that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf. See Section 3.2.2.4.	If at least one dNSName instance is present in the permittedSubtrees, the CA MAY indicate one or more subordinate domains to be excluded.	If no dNSName instance is present in the permittedSubtrees, then the CA MUST include a zero-length dNSName to indicate no domain names are permitted.
iPAddress	MUST	The CA MUST confirm that the Applicant has been assigned the iPAddress range or has been authorized by the assigner to act on the asignee's behalf. See Section 0.	If at least one iPAddress instance is present in the permittedSubtrees, the CA MAY indicate one or more subdivisions of those ranges to be excluded.	If no IPv4 iPAddress is present in the permittedSubtrees, the CA MUST include an iPAddress of 8 zero octets, indicating the IPv4 range of 0.0.0.0/0 being excluded. If no IPv6 iPAddress is present in the permittedSubtrees, the CA MUST include an iPAddress of 32 zero octets, indicating the IPv6 range of ::0/0 being excluded.
directoryName	MUST	The CA MUST confirm the Applicant's and/or Subsidiary's name attributes such that all certificates issued will comply with the relevant	It is NOT RECOMMENDED to include values within excludedSubtrees.	The CA MUST include a value within permittedSubtrees, and as such, this does not apply.

		Certificate Profile (see Section 7.1.2), including Name Forms (See Section 7.1.4).		See the Excluded Subtrees requirements for more.
otherName	NOT RECOMMENDED	See below	See below	See below
Any other value	MUST NOT	-	-	-

Any otherName, if present:

1. MUST apply in the context of the public Internet, unless:
   a. the type-id falls within an OID arc for which the Applicant demonstrates ownership, or,
   b. the Applicant can otherwise demonstrate the right to assert the data in a public context.
2. MUST NOT include semantics that will mislead the Relying Party about certificate information verified by the CA.
3. MUST be DER encoded according to the relevant ASN.1 module defining the otherName type-id and value.

CAs SHALL NOT include additional names unless the CA is aware of a reason for including the data in the Certificate.

7.1.2.6 TLS SUBORDINATE CA CERTIFICATE PROFILE

Field	Description
tbsCertificate	
version	MUST be v3(2)
serialNumber	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature	See Section 7.1.3.2
issuer	MUST be byte-for-byte identical to the subject field of the Issuing CA. See Section 7.1.4.1
validity	See Section 7.1.2.10.1
subject	See Section 7.1.2.10.2
subjectPublicKeyInfo	See Section 7.1.3.1
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present
extensions	See Section 7.1.2.6.1
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.6.1 TLS SUBORDINATE CA EXTENSIONS

Extension	Presence	Critical	Description
authorityKeyIdentifier	MUST	N	See Section 7.1.2.11.1
basicConstraints	MUST	Y	See Section 7.1.2.10.4
certificatePolicies	MUST	N	See Section 0
crlDistributionPoints	MUST	N	See Section 7.1.2.11.2
keyUsage	MUST	Y	See Section 7.1.2.10.7
subjectKeyIdentifier	MUST	N	See Section 7.1.2.11.4
extKeyUsage	MUST[4]	N	See Section 7.1.2.10.6
authorityInformationAccess	SHOULD	N	See Section 7.1.2.10.3
nameConstraints	MAY	*[5]	See Section 0
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

The profile of TunTrust Services CA is available in Appendix A of this CP/CPS.

7.1.2.7 SUBSCRIBER (SERVER) CERTIFICATE PROFILE

Field	Description
tbsCertificate	
version	MUST be v3(2)
serialNumber	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature	See Section 7.1.3.2
issuer	MUST be byte-for-byte identical to the subject field of the Issuing CA. See Section 7.1.4.1
validity	
notBefore	A value within 48 hours of the certificate signing operation.
notAfter	See Section 6.3.2
subject	See Section 7.1.2.7.1
subjectPublicKeyInfo	See Section 7.1.3.1
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present

[4] While RFC 5280, Section 4.2.1.12 notes that this extension will generally only appear within end-entity certificates, these Requirements make use of this extension to further protect relying parties by limiting the scope of CA Certificates, as implemented by a number of Application Software Suppliers.

[5] See Section 0 for further requirements, including regarding criticality of this extension.

extensions	See Section 7.1.2.7.6
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.7.1 Subscriber Certificate Types

There are four types of Subscriber Certificates that may be issued, which vary based on the amount of Subject Information that is included. Each of these certificate types shares a common profile, with three exceptions: the subject name fields that may occur, how those fields are validated, and the contents of the certificatePolicies extension.

Type	Description
Domain Validated (DV)	See Section 7.1.2.7.2
Individual Validated (IV)	See Section 7.1.2.7.3
Organization Validated (OV)	See Section 7.1.2.7.4
Extended Validation (EV)	See Section 7.1.2.7.5

Note: Although each Subscriber Certificate type varies in Subject Information, all Certificates provide the same level of assurance of the device identity (domain name and/or IP address). TunTrust issues OV SSL Certificates with this hierarchy. Refer to Appendix B for TunTrust Subscriber Certificate Profile.

7.1.2.7.2 Domain Validated

Not Applicable. TunTrust issues only OV SSL Certificates using this hierarchy.

7.1.2.7.3 Individual Validated

Not Applicable. TunTrust issues only OV SSL Certificates using this hierarchy.

7.1.2.7.4 Organization Validated

For a Subscriber Certificate to be Organization Validated, it MUST meet the following profile:

Field	Requirements
subject	See following table.
certificatePolicies	MUST be present. MUST assert the Reserved Certificate Policy Identifier of 2.23.140.1.2.2 as a policyIdentifier. See Section 7.1.2.7.9.
All other extensions	See Section 7.1.2.7.6

All subject names MUST be encoded as specified in Section 7.1.4.

The following table details the acceptable AttributeTypes that may appear within the type field of an AttributeTypeAndValue, as well as the contents permitted within the value field.

Organization Validated subject Attributes

Attribute Name	Presence	Value	Verification

domainComponent	MAY	If present, this field MUST contain a Domain Label from a Domain Name. The domainComponent fields for the Domain Name MUST be in a single ordered sequence containing all Domain Labels from the Domain Name. The Domain Labels MUST be encoded in the reverse order to the on-wire representation of domain names in the DNS protocol, so that the Domain Label closest to the root is encoded first. Multiple instances MAY be present.	[Section 3.2]
countryName	MUST	The two-letter ISO 3166-1 country code for the country associated with the Subject. If a Country is not represented by an official ISO 3166-1 country code, the CA MUST specify the ISO 3166-1 user-assigned code of XX, indicating that an official ISO 3166-1 alpha-2 code has not been assigned.	Section 3.2.2.1
stateOrProvinceName	MUST / MAY	MUST be present if localityName is absent, MAY be present otherwise. If present, MUST contain the Subject's state or province information.	Section 3.2.2.1
localityName	MUST / MAY	MUST be present if stateOrProvinceName is absent, MAY be present otherwise. If present, MUST contain the Subject's locality information.	Section 3.2.2.1
postalCode	NOT RECOMMENDED	If present, MUST contain the Subject's zip or postal information.	Section 3.2.2.1
streetAddress	NOT RECOMMENDED	If present, MUST contain the Subject's street address information. Multiple instances MAY be present.	Section 3.2.2.1
organizationName	MUST	The Subject's name and/or DBA/tradename. The CA MAY include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g. if the official record shows "Company Name Incorporated", the CA MAY use "Company Name Inc." or "Company Name". If both are included, the DBA/tradename SHALL appear first,	Section 3.2.2.1

		followed by the Subject's name in parentheses.	
surname	MUST NOT	-	-
givenName	MUST NOT	-	-
organizationalUnitName	MUST NOT	-	-
commonName	NOT RECOMMENDED	If present, MUST contain a value derived from the subjectAltName extension according to Section 7.1.4.3.	
Any other attribute	NOT RECOMMENDED	-	See Section 7.1.4.3

Subject attributes don't contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.2.7.5 Extended Validation

Not Applicable. TunTrust issues only OV SSL Certificates using this hierarchy.

7.1.2.7.6 Subscriber Certificate Extensions

Extension	Presence	Critical	Description
authorityInformationAccess	MUST	N	See Section 7.1.2.7.7
authorityKeyIdentifier	MUST	N	See Section 7.1.2.11.1
certificatePolicies	MUST	N	See Section 7.1.2.7.9
extKeyUsage	MUST	N	See Section 7.1.2.7.10
subjectAltName	MUST	*	See Section 7.1.2.7.12
nameConstraints	MUST NOT	-	-
keyUsage	SHOULD	Y	See Section 7.1.2.7.11
basicConstraints	MAY	Y	See Section 0
crlDistributionPoints	*	N	See Section 7.1.2.11.2
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
subjectKeyIdentifier	NOT RECOMMENDED	N	See Section 7.1.2.11.4
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

Notes:

- Whether or not the subjectAltName extension should be marked Critical depends on the contents of the Certificate's subject field, as detailed in Section 7.1.2.7.12.
- Whether or not the CRL Distribution Points extension must be present depends on 1) whether the Certificate includes an Authority Information Access extension with an id-ad-ocsp accessMethod and 2) the Certificate's validity period, as detailed in Section 7.1.2.11.2.

7.1.2.7.7 Subscriber Certificate Authority Information Access

The AuthorityInfoAccessSyntax MUST contain one or more AccessDescriptions. Each AccessDescription MUST only contain a permitted accessMethod, as detailed below, and each accessLocation MUST be encoded as the specified GeneralName type.

The AuthorityInfoAccessSyntax MAY contain multiple AccessDescriptions with the same accessMethod, if permitted for that accessMethod. When multiple AccessDescriptions are present with the same accessMethod, each accessLocation MUST be unique, and each AccessDescription MUST be ordered in priority for that accessMethod, with the most-preferred accessLocation being the first AccessDescription. No ordering requirements are given for AccessDescriptions that contain different accessMethods, provided that previous requirement is satisfied.

Access Method	Access Location	Presence	Maximum	Description
id-ad-ocsp(OID: 1.3.6.1.5.5.7.48.1)	uniformResourceIdentifier	MAY	*	A HTTP URL of the Issuing CA's OCSP responder.
id-ad-caIssuers(OID: 1.3.6.1.5.5.7.48.2)	uniformResourceIdentifier	SHOULD	*	A HTTP URL of the Issuing CA's certificate.
Any other value	-	MUST NOT	-	No other accessMethods may be used.

7.1.2.7.8 Subscriber Certificate Basic Constraints

Field	Description
cA	MUST be FALSE
pathLenConstraint	MUST NOT be present

7.1.2.7.9 Subscriber Certificate Certificate Policies

If present, the Certificate Policies extension MUST contain at least one PolicyInformation. Each PolicyInformation MUST match the following profile:

Field	Presence	Contents
policyIdentifier	MUST	One of the following policy identifiers:

A Reserved Certificate Policy Identifier	MUST	The Reserved Certificate Policy Identifier (see Section 7.1.6.1) associated with the given Subscriber Certificate type (see Section 7.1.2.7.1).
anyPolicy	MUST NOT	The anyPolicy Policy Identifier MUST NOT be present.
Any other identifier	MAY	If present, MUST be defined and documented in the CA's Certificate Policy and/or Certification Practice Statement.
policyQualifiers	NOT RECOMMENDED	If present, MUST contain only permitted policyQualifiers from the table below.

This Profile RECOMMENDS that the first PolicyInformation value within the Certificate Policies extension contains the Reserved Certificate Policy Identifier (see 7.1.6.1)[6] . Regardless of the order of PolicyInformation values, the Certificate Policies extension MUST contain exactly one Reserved Certificate Policy Identifier.

Permitted policyQualifiers

Qualifier ID	Presence	Field Type	Contents
id-qt-cps (OID: 1.3.6.1.5.5.7.2.1)	MAY	IA5String	The HTTP or HTTPS URL for the Issuing CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the Issuing CA.
Any other qualifier	MUST NOT	-	-

7.1.2.7.10 Subscriber Certificate Extended Key Usage

Key Purpose	OID	Presence
id-kp-serverAuth	1.3.6.1.5.5.7.3.1	MUST
id-kp-clientAuth	1.3.6.1.5.5.7.3.2	MAY
id-kp-codeSigning	1.3.6.1.5.5.7.3.3	MUST NOT
id-kp-emailProtection	1.3.6.1.5.5.7.3.4	MUST NOT
id-kp-timeStamping	1.3.6.1.5.5.7.3.8	MUST NOT
id-kp-OCSPSigning	1.3.6.1.5.5.7.3.9	MUST NOT
anyExtendedKeyUsage	2.5.29.37.0	MUST NOT
Precertificate Signing Certificate	1.3.6.1.4.1.11129.2.4.4	MUST NOT
Any other value	-	NOT RECOMMENDED

7.1.2.7.11 Subscriber Certificate Key Usage

[6] Although RFC 5280 allows PolicyInformations to appear in any order, several client implementations have implemented logic that considers the policyIdentifier that matches a given filter. As such, ensuring the Reserved Certificate Policy Identifier is the first PolicyInformation reduces the risk of interoperability challenges.

The acceptable Key Usage values vary based on whether the Certificate's subjectPublicKeyInfo identifies an RSA public key or an ECC public key. CAs MUST ensure the Key Usage is appropriate for the Certificate Public Key. TunTrust only uses RSA Public Keys in this CA hierarchy.

Key Usage for RSA Public Keys

Key Usage	Permitted	Required
digitalSignature	Y	SHOULD
nonRepudiation	N	–
keyEncipherment	Y	MAY
dataEncipherment	Y	NOT RECOMMENDED
keyAgreement	N	–
keyCertSign	N	–
cRLSign	N	–
encipherOnly	N	–
decipherOnly	N	–

Note: At least one Key Usage MUST be set for RSA Public Keys. The digitalSignature bit is REQUIRED for use with modern protocols, such as TLS 1.3, and secure ciphersuites, while the keyEncipherment bit MAY be asserted to support older protocols, such as TLS 1.2, when using insecure ciphersuites. Subscribers MAY wish to ensure key separation to limit the risk from such legacy protocols, and thus a CA MAY issue a Subscriber certificate that only asserts the keyEncipherment bit. For most Subscribers, the digitalSignature bit is sufficient, while Subscribers that want to mix insecure and secure ciphersuites with the same algorithm may choose to assert both digitalSignature and keyEncipherment within the same certificate, although this is NOT RECOMMENDED. The dataEncipherment bit is currently permitted, although setting it is NOT RECOMMENDED, as it is a Pending Prohibition (https://github.com/cabforum/servercert/issues/384). Therefore, TunTrust does not does not use the dataEncipherment bit.

7.1.2.7.12 Subscriber Certificate Subject Alternative Name

For Subscriber Certificates, the Subject Alternative Name MUST be present and MUST contain at least one dNSName or iPAddress GeneralName. See below for further requirements about the permitted fields and their validation requirements.

If the subject field of the certificate is an empty SEQUENCE, this extension MUST be marked critical, as specified in RFC 5280, Section 4.2.1.6. Otherwise, this extension MUST NOT be marked critical.

GeneralName within a subjectAltName extension

Name Type	Permitted	Validation
otherName	N	-
rfc822Name	N	-
dNSName	Y	The entry MUST contain either a Fully-Qualified Domain Name or Wildcard Domain Name that the CA has validated in accordance with Section 3.2.2.4. Wildcard Domain Names MUST be validated for consistency with Section 3.2.2.6. The entry MUST NOT contain an Internal Name. The Fully-Qualified

		Domain Name or the FQDN portion of the Wildcard Domain Name contained in the entry MUST be composed entirely of P-Labels or Non-Reserved LDH Labels joined together by a U+002E FULL STOP (".") character. The zero-length Domain Label representing the root zone of the Internet Domain Name System MUST NOT be included (e.g. "example.com" MUST be encoded as "example.com" and MUST NOT be encoded as "example.com.").
x400Address	N	-
directoryName	N	-
ediPartyName	N	-
uniformResourceIdentifier	N	-
iPAddress	Y	The entry MUST contain the IPv4 or IPv6 address that the CA has confirmed the Applicant controls or has been granted the right to use through a method specified in Section 0. The entry MUST NOT contain a Reserved IP Address.
registeredID	N	-

Note: As an explicit exception from RFC 5280, P-Labels are permitted to not conform to IDNA 2003. The Baseline Requirements allow for the inclusion of P-Labels that do not conform with IDNA 2003 to support newer versions of the Unicode character repertoire, among other improvements to the various IDNA standards.

7.1.2.8 OCSP RESPONDER CERTIFICATE PROFILE

If the Issuing CA does not directly sign OCSP responses, it MAY make use of an OCSP Authorized Responder, as defined by RFC 6960, Section 4.2.2.2. The Issuing CA of the Responder MUST be the same as the Issuing CA for the Certificates it provides responses for.

Refer to Appendix D for TunTrust OCSP profile.

Field	Description
tbsCertificate	
version	MUST be v3(2)
serialNumber	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature	See Section 7.1.3.2
issuer	MUST be byte-for-byte identical to the subject field of the Issuing CA. See Section 7.1.4.1
validity	See Section 7.1.2.8.1
subject	See Section 7.1.2.10.2
subjectPublicKeyInfo	See Section 7.1.3.1
issuerUniqueID	MUST NOT be present

subjectUniqueID	MUST NOT be present
extensions	See Section 7.1.2.8.2
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.8.1 OCSP Responder Validity

Field	Minimum	Maximum
notBefore	One day prior to the time of signing	The time of signing
notAfter	The time of signing	Unspecified

7.1.2.8.2 OCSP Responder Validity

Extension	Presence	Critical	Description
authorityKeyIdentifier	MUST	N	See Section 7.1.2.11.1
extKeyUsage	MUST	-	See Section 7.1.2.8.5
id-pkix-ocsp-nocheck	MUST	N	See Section 0
keyUsage	MUST	Y	See Section 7.1.2.8.7
basicConstraints	MAY	Y	See Section 7.1.2.8.4
nameConstraints	MUST NOT	-	-
subjectAltName	MUST NOT	-	-
subjectKeyIdentifier	SHOULD	N	See Section 7.1.2.11.4
authorityInformationAccess	NOT RECOMMENDED	N	See Section 7.1.2.8.3
certificatePolicies	SHOULD NOT	N	See Section 7.1.2.8.8
crlDistributionPoints	MUST NOT	N	See Section 7.1.2.11.2
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

7.1.2.8.3 OCSP Responder Authority Information Access

For OCSP Responder certificates, this extension is NOT RECOMMENDED, as the Relying Party should already possess the necessary information. In order to validate the given Responder certificate, the Relying Party must have access to the Issuing CA's certificate, eliminating the need to provide id-ad-caIssuers. Similarly, because of the requirement for an OCSP Responder certificate to include the id-pkix-ocsp-nocheck extension, it is not necessary to provide id-ad-ocsp, as such responses will not be checked by Relying Parties.

If present, the AuthorityInfoAccessSyntax MUST contain one or more AccessDescriptions. Each AccessDescription MUST only contain a permitted accessMethod, as detailed below, and each AuthorityInfoAccessSyntax MUST contain all required AccessDescriptions.

Access Method	Access Location	Presence	Maximum	Description

id-ad-ocsp(OID: 1.3.6.1.5.5.7.48.1)	uniformResourceIdentifier	NOT RECOMMENDED	*	A HTTP URL of the Issuing CA's OCSP responder.
Any other value	-	MUST NOT	-	No other accessMethods may be used.

7.1.2.8.4 OCSP RESPONDER BASIC CONSTRAINTS

OCSP Responder certificates MUST NOT be CA certificates. The issuing CA may indicate this one of two ways: by omission of the basicConstraints extension, or through the inclusion of a basicConstraints extension that sets the cA boolean to FALSE.

Field	Description
cA	MUST be FALSE
pathLenConstraint	MUST NOT be present

Note: Due to DER encoding rules regarding the encoding of DEFAULT values within OPTIONAL fields, a basicConstraints extension that sets the cA boolean to FALSE MUST have an extnValue OCTET STRING which is exactly the hex-encoded bytes 3000, the encoded representation of an empty ASN.1 SEQUENCE value.

7.1.2.8.5 OCSP RESPONDER EXTENDED KEY USAGE

Key Purpose	OID	Presence
id-kp-OCSPSigning	1.3.6.1.5.5.7.3.9	MUST
Any other value	-	MUST NOT

7.1.2.8.6 OCSP RESPONDER ID-PKIX-OCSP-NOCHECK

The CA MUST include the id-pkix-ocsp-nocheck extension (OID: 1.3.6.1.5.5.7.48.1.5).

This extension MUST have an extnValue OCTET STRING which is exactly the hex-encoded bytes 0500, the encoded representation of the ASN.1 NULL value, as specified in RFC 6960, Section 4.2.2.2.1.

7.1.2.8.7 OCSP RESPONDER KEY USAGE

Key Usage	Permitted	Required
digitalSignature	Y	Y
nonRepudiation	N	–
keyEncipherment	N	–
dataEncipherment	N	–
keyAgreement	N	–
keyCertSign	N	–
cRLSign	N	–
encipherOnly	N	–
decipherOnly	N	–

7.1.2.8.8 OCSP RESPONDER CERTIFICATE POLICIES

If present, the Certificate Policies extension MUST contain at least one PolicyInformation. Each PolicyInformation MUST match the following profile:

Permitted policyQualifiers

Field	Presence	Contents
`policyIdentifier`	MUST	One of the following policy identifiers:
A Reserved Certificate Policy Identifier	NOT RECOMMENDED	
`anyPolicy`	NOT RECOMMENDED	
Any other identifier	NOT RECOMMENDED	If present, MUST be defined by the CA and documented by the CA in its Certificate Policy and/or Certification Practice Statement.
`policyQualifiers`	NOT RECOMMENDED	If present, MUST contain only permitted `policyQualifiers` from the table below.

Qualifier ID	Presence	Field Type	Contents
`id-qt-cps` (OID: 1.3.6.1.5.5.7.2.1)	MAY	`IA5String`	The HTTP or HTTPS URL for the Issuing CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the Issuing CA.
Any other qualifier	MUST NOT	-	-

Note: Because the Certificate Policies extension may be used to restrict the applicable usages for a Certificate, incorrect policies may result in OCSP Responder Certificates that fail to successfully validate, resulting in invalid OCSP Responses. Including the anyPolicy policy can reduce this risk, but add to client processing complexity and interoperability issues.

7.1.2.9 PRECERTIFICATE PROFILE

A Precertificate is a signed data structure that can be submitted to a Certificate Transparency log, as defined by RFC 6962. A Precertificate appears structurally identical to a Certificate, with the exception of a special critical poison extension in the extensions field, with the OID of 1.3.6.1.4.1.11129.2.4.3. This extension ensures that the Precertificate will not be accepted as a Certificate by clients conforming to RFC 5280. The existence of a signed Precertificate can be treated as evidence of a corresponding Certificate also existing, as the signature represents a binding commitment by the CA that it may issue such a Certificate.

A Precertificate is created after a CA has decided to issue a Certificate, but prior to the actual signing of the Certificate.

Once a Precertificate is signed, relying parties are permitted to treat this as a binding commitment from the CA of the intent to issue a corresponding Certificate, or more commonly, that a corresponding Certificate exists. A Certificate is said to be corresponding to a Precertificate based upon the value of the tbsCertificate contents, as transformed by the process defined in RFC 6962, Section 3.2.

This profile describes the transformations that are permitted to a Certificate to construct a Precertificate. TunTrust does not issue a Precertificate unless it is willing to issue a corresponding Certificate, regardless of whether it has done so. Similarly, TunTrust CAs do not issue a Precertificate unless the corresponding Certificate conforms to the Baseline Requirements, regardless of whether TunTrust CAs sign the corresponding Certificate.

A Precertificate is issued directly by TunTrust Issuing CA.

Field	Description
`tbsCertificate`	
`version`	Encoded value MUST be byte-for-byte identical to the `version` field of the Certificate
`serialNumber`	Encoded value MUST be byte-for-byte identical to the `serialNumber` field of the Certificate
`signature`	Encoded value MUST be byte-for-byte identical to the `signature` field of the Certificate
`issuer`	Encoded value MUST be byte-for-byte identical to the `issuer` field of the Certificate
`validity`	Encoded value MUST be byte-for-byte identical to the `validity` field of the Certificate
`subject`	Encoded value MUST be byte-for-byte identical to the `subject` field of the Certificate
`subjectPublicKeyInfo`	Encoded value MUST be byte-for-byte identical to the `subjectPublicKeyInfo` field of the Certificate
`issuerUniqueID`	Encoded value MUST be byte-for-byte identical to the `issuerUniqueID` field of the Certificate, or omitted if omitted in the Certificate
`subjectUniqueID`	Encoded value MUST be byte-for-byte identical to the `subjectUniqueID` field of the Certificate, or omitted if omitted in the Certificate
`extensions`	See Section 7.1.2.9.1
`signatureAlgorithm`	Encoded value MUST be byte-for-byte identical to the `tbsCertificate.signature`.
`signature`	

7.1.2.9.1 PRECERTIFICATE PROFILE EXTENSIONS - DIRECTLY ISSUED

These extensions apply in the context of a Precertificate directly issued from a CA, and not from a Precertificate Signing CA Certificate, as defined in Section 7.1.2.4.

Extension	Presence	Critical	Description
Precertificate Poison (OID: 1.3.6.1.4.1.11129.2.4.3)	MUST	Y	See Section 7.1.2.9.3

Signed Certificate Timestamp List	MUST NOT	-	
Any other extension	*	*	The order, criticality, and encoded values of all other extensions MUST be byte-for-byte identical to the `extensions` field of the Certificate

Note: This requirement is expressing that if the Precertificate Poison extension is removed from the Precertificate, and the Signed Certificate Timestamp List is removed from the certificate, the contents of the extensions field MUST be byte-for-byte identical to the Certificate.

7.1.2.9.2 PRECERTIFICATE PROFILE EXTENSIONS - PRECERTIFICATE CA ISSUED

Not Applicable.

7.1.2.9.3 PRECERTIFICATE POISON

The Precertificate MUST contain the Precertificate Poison extension (OID: 1.3.6.1.4.1.11129.2.4.3).

This extension MUST have an extnValue OCTET STRING which is exactly the hex-encoded bytes 0500, the encoded representation of the ASN.1 NULL value, as specified in RFC 6962, Section 3.1.

7.1.2.9.4 PRECERTIFICATE AUTHORITY KEY IDENTIFIER

Not Applicable. TunTrust does not have a Precertificate Signing CA.

7.1.2.10 COMMON CA FIELDS

This section contains several fields that are common among multiple CA Certificate profiles. However, these fields may not be common among all CA Certificate profiles. Before issuing a certificate, the CA MUST ensure the certificate contents, including the contents of each field, complies in whole with all of the requirements of at least one Certificate Profile documented in Section 7.1.2.

7.1.2.10.1 CA CERTIFICATE VALIDITY

Field	Minimum	Maximum
`notBefore`	One day prior to the time of signing	The time of signing
`notAfter`	The time of signing	Unspecified

7.1.2.10.2 CA CERTIFICATE NAMING

All subject names MUST be encoded as specified in Section 7.1.4.

The following table details the acceptable AttributeTypes that may appear within the type field of an AttributeTypeAndValue, as well as the contents permitted within the value field.

Attribute Name	Presence	Value	Verification
`countryName`	MUST	The two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.	Section 3.2.2.3

stateOrProvinceName	MAY	If present, the CA's state or province information.	Section 3.2.2.1
localityName	MAY	If present, the CA's locality.	Section 3.2.2.1
postalCode	MAY	If present, the CA's zip or postal information.	Section 3.2.2.1
streetAddress	MAY	If present, the CA's street address. Multiple instances MAY be present.	Section 3.2.2.1
organizationName	MUST	The CA's name or DBA. The CA MAY include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g. if the official record shows "Company Name Incorporated", the CA MAY use "Company Name Inc." or "Company Name".	Section 3.2.2.2
organizationalUnitName	This attribute MUST NOT be included in Root CA Certificates defined in Section 7.1.2.1 or TLS Subordinate CA Certificates defined in Section 7.1.2.5 or Technically-Constrained TLS Subordinate CA Certificates defined in Section 7.1.2.6. This attribute SHOULD NOT be included in other types of CA Certificates.	-	-
commonName	MUST	The contents SHOULD be an identifier for the certificate such that the certificate's Name is unique across all	

		certificates issued by the issuing certificate.	
Any other attribute	NOT RECOMMENDED	-	See Section 7.1.4.3

7.1.2.10.3 CA Certificate Authority Information Access

If present, the AuthorityInfoAccessSyntax MUST contain one or more AccessDescriptions. Each AccessDescription MUST only contain a permitted accessMethod, as detailed below, and each accessLocation MUST be encoded as the specified GeneralName type.

The AuthorityInfoAccessSyntax MAY contain multiple AccessDescriptions with the same accessMethod, if permitted for that accessMethod. When multiple AccessDescriptions are present with the same accessMethod, each accessLocation MUST be unique, and each AccessDescription MUST be ordered in priority for that accessMethod, with the most-preferred accessLocation being the first AccessDescription. No ordering requirements are given for AccessDescriptions that contain different accessMethods, provided that previous requirement is satisfied.

Access Method	Access Location	Presence	Maximum	Description
`id-ad-ocsp(OID1.3.6.1.5.5.7.48.1)`	`uniformResourceIdentifier`	MAY	*	A HTTP URL of the Issuing CA's OCSP responder.
`id-ad-caIssuers(OID: 1.3.6.1.5.5.7.48.2)`	`uniformResourceIdentifier`	MAY	*	A HTTP URL of the Issuing CA's certificate.
Any other value	-	MUST NOT	-	No other `accessMethods` may be used.

7.1.2.10.4 CA Certificate Basic Constraints

Field	Description
`cA`	MUST be set TRUE
`pathLenConstraint`	MAY be present

7.1.2.10.5 CA Certificate Certificate Policies

If present, the Certificate Policies extension MUST contain at least one PolicyInformation. Each PolicyInformation MUST match the following profile:

No Policy Restrictions (Affiliated CA)

Field	Presence	Contents
`policyIdentifier`	MUST	When the Issuing CA wishes to express that there are no policy restrictions, the Subordinate CA

		MUST be an Affiliate of the Issuing CA. The Certificate Policies extension MUST contain only a single `PolicyInformation` value, which MUST contain the `anyPolicy` Policy Identifier.
`anyPolicy`	MUST	
`policyQualifiers`	NOT RECOMMENDED	If present, MUST contain only permitted `policyQualifiers` from the table below.

Policy Restricted

Field	Presence	Contents
`policyIdentifier`	MUST	One of the following policy identifiers:
A Reserved Certificate Policy Identifier	MUST	The CA MUST include exactly one Reserved Certificate Policy Identifier (see Section 7.1.6.1) associated with the given Subscriber Certificate type (see Section 7.1.2.7.1) directly or transitively issued by this Certificate.
`anyPolicy`	MUST NOT	The `anyPolicy` Policy Identifier MUST NOT be present.
Any other identifier	MAY	If present, MUST be defined by the CA and documented by the CA in its Certificate Policy and/or Certification Practice Statement.
`policyQualifiers`	NOT RECOMMENDED	If present, MUST contain only permitted `policyQualifiers` from the table below.

The Policy Restricted profile RECOMMENDS that the first PolicyInformation value within the Certificate Policies extension contains the Reserved Certificate Policy Identifier (see 7.1.6.1)[7]. Regardless of the order of PolicyInformation values, the Certificate Policies extension MUST contain exactly one Reserved Certificate Policy Identifier.

Note: policyQualifiers is NOT RECOMMENDED to be present in any Certificate issued under this Certificate Profile because this information increases the size of the Certificate without providing any value to a typical Relying Party, and the information may be obtained by other means when necessary. Therefore, the policyQualifiers is not present in TunTrust CA Certificates.

[7] Although RFC 5280 allows PolicyInformations to appear in any order, several client implementations have implemented logic that considers the policyIdentifier that matches a given filter. As such, ensuring the Reserved Certificate Policy Identifier is the first PolicyInformation reduces the risk of interoperability challenges.

7.1.2.10.6 CA Certificate Extended Key Usage

Key Purpose	OID	Presence
id-kp-serverAuth	1.3.6.1.5.5.7.3.1	MUST
id-kp-clientAuth	1.3.6.1.5.5.7.3.2	MAY
id-kp-codeSigning	1.3.6.1.5.5.7.3.3	MUST NOT
id-kp-emailProtection	1.3.6.1.5.5.7.3.4	MUST NOT
id-kp-timeStamping	1.3.6.1.5.5.7.3.8	MUST NOT
id-kp-OCSPSigning	1.3.6.1.5.5.7.3.9	MUST NOT
anyExtendedKeyUsage	2.5.29.37.0	MUST NOT
Precertificate Signing Certificate	1.3.6.1.4.1.11129.2.4.4	MUST NOT
Any other value	-	NOT RECOMMENDED

7.1.2.10.7 CA Certificate Key Usage

Key Usage	Permitted	Required
digitalSignature	Y	N[8]
nonRepudiation	N	–
keyEncipherment	N	–
dataEncipherment	N	–
keyAgreement	N	–
keyCertSign	Y	Y
cRLSign	Y	Y
encipherOnly	N	–
decipherOnly	N	–

7.1.2.10.8 CA Certificate Name Constraints

If present, the Name Constraints extension MUST be encoded as follows. As an explicit exception from RFC 5280, this extension SHOULD be marked critical, but MAY be marked non-critical if compatability with certain legacy applications that do not support Name Constraints is necessary.

nameConstraints requirements

Field	Description
permittedSubtrees	
GeneralSubtree	The requirements for a GeneralSubtree that appears within a permittedSubtrees.
base	See following table.

[8] If a CA Certificate does not assert the digitalSignature bit, the CA Private Key MUST NOT be used to sign an OCSP Response. See Section 7.3 for more information.

minimum	MUST NOT be present.
maximum	MUST NOT be present.
excludedSubtrees	
GeneralSubtree	The requirements for a GeneralSubtree that appears within a permittedSubtrees.
base	See following table.
minimum	MUST NOT be present.
maximum	MUST NOT be present.

The following table contains the requirements for the GeneralName that appears within the base of a GeneralSubtree in either the permittedSubtrees or excludedSubtrees.

GeneralName requirements for the base field

Name Type	Presence	Permitted Subtrees	Excluded Subtrees
dNSName	MAY	The CA MUST confirm that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf. See Section 3.2.2.4.	If at least one dNSName instance is present in the permittedSubtrees, the CA MAY indicate one or more subordinate domains to be excluded.
iPAddress	MAY	The CA MUST confirm that the Applicant has been assigned the iPAddress range or has been authorized by the assigner to act on the asignee's behalf. See Section 0.	If at least one iPAddress instance is present in the permittedSubtrees, the CA MAY indicate one or more subdivisions of those ranges to be excluded.
directoryName	MAY	The CA MUST confirm the Applicant's and/or Subsidiary's name attributes such that all certificates issued will comply with the relevant Certificate Profile (see Section 7.1.2), including Name Forms (See Section 7.1.4).	It is NOT RECOMMENDED to include values within excludedSubtrees.
rfc822Name	NOT RECOMMENDED	The CA MAY constrain to a mailbox, a particular host, or any address within a domain, as specified within RFC 5280, Section 4.2.1.10. For each host, domain, or Domain portion of a Mailbox (as specified within RFC 5280, Section 4.2.1.6), the CA MUST confirm that the Applicant has	If at least one rfc822Name instance is present in the permittedSubtrees, the CA MAY indicate one or more mailboxes, hosts, or domains to be excluded.

		registered the domain or has been authorized by the domain registrant to act on the registrant's behalf. See Section 3.2.2.4.	
otherName	NOT RECOMMENDED	See below	See below
Any other value	NOT RECOMMENDED	-	-

Any otherName, if present:

1. MUST apply in the context of the public Internet, unless:
   a. the type-id falls within an OID arc for which the Applicant demonstrates ownership, or,
   b. the Applicant can otherwise demonstrate the right to assert the data in a public context.
2. MUST NOT include semantics that will mislead the Relying Party about certificate information verified by the CA.
3. MUST be DER encoded according to the relevant ASN.1 module defining the otherName type-id and value.

TunTrust does not include additional names in the Certificate.

7.1.2.11 Common Certificate Fields

This section contains several fields that are common among multiple certificate profiles. However, these fields may not be common among all certificate profiles. Before issuing a certificate, the CA MUST ensure the certificate contents, including the contents of each field, complies in whole with all of the requirements of at least one Certificate Profile documented in Section 7.1.2.

7.1.2.11.1 Authority Key Identifier

Field	Description
keyIdentifier	MUST be present. MUST be identical to the subjectKeyIdentifier field of the Issuing CA.
authorityCertIssuer	MUST NOT be present
authorityCertSerialNumber	MUST NOT be present

7.1.2.11.2 CRL Distribution Points

The CRL Distribution Points extension MUST be present in:

- Subordinate CA Certificates; and

- Subscriber Certificates that

  1) do not qualify as "Short-lived Subscriber Certificates" and

  2) do not include an Authority Information Access extension with an id-ad-ocsp accessMethod.

The CRL Distribution Points extension SHOULD NOT be present in Root CA Certificates.

The CRL Distribution Points extension is OPTIONAL in Short-lived Subscriber Certificates.

The CRL Distribution Points extension MUST NOT be present in OCSP Responder Certificates.

When present, the CRL Distribution Points extension MUST contain at least one DistributionPoint; containing more than one is NOT RECOMMENDED. All DistributionPoint items must be formatted as follows:

DistributionPoint profile

Field	Presence	Description
`distributionPoint`	MUST	The `DistributionPointName` MUST be a `fullName` formatted as described below.
`reasons`	MUST NOT	
`cRLIssuer`	MUST NOT	

A fullName MUST contain at least one GeneralName; it MAY contain more than one. All GeneralNames MUST be of type uniformResourceIdentifier, and the scheme of each MUST be “http”. The first GeneralName must contain the HTTP URL of the Issuing CA’s CRL service for this certificate.

7.1.2.11.3 Signed Certificate Timestamp List

If present, the Signed Certificate Timestamp List extension contents MUST be an OCTET STRING containing the encoded SignedCertificateTimestampList, as specified in RFC 6962, Section 3.3.

Each SignedCertificateTimestamp included within the SignedCertificateTimestampList MUST be for a PreCert LogEntryType that corresponds to the current certificate.

7.1.2.11.4 Subject Key Identifier

If present, the subjectKeyIdentifier MUST be set as defined within RFC 5280, Section 4.2.1.2. The CA MUST generate a subjectKeyIdentifier that is unique within the scope of all Certificates it has issued for each unique public key (the subjectPublicKeyInfo field of the tbsCertificate). For example, CAs may generate the subject key identifier using an algorithm derived from the public key, or may generate a sufficiently-large unique number, such as by using a CSPRNG.

7.1.2.11.5 Other Extensions

All extensions and extension values not directly addressed by the applicable certificate profile:

1. MUST apply in the context of the public Internet, unless:
   a. the extension OID falls within an OID arc for which the Applicant demonstrates ownership, or,
   b. the Applicant can otherwise demonstrate the right to assert the data in a public context.
2. MUST NOT include semantics that will mislead the Relying Party about certificate information verified by the CA (such as including an extension that indicates a Private Key is stored on a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).
3. MUST be DER encoded according to the relevant ASN.1 module defining the extension and extension values.

TunTrust does not include additional names in the Certificate.

7.1.3 Algorithm object identifiers

All signing algorithms used by TunTrust are sha256WithRSAEncryption. TunTrust CA does not, and never has, used SHA-1 as a component of any signature algorithm on a certificate.

Algorithms OID are conforming to IETF RFC 3279 and RFC 5280.

7.1.3.1 SUBJECTPUBLICKEYINFO

TunTrust indicates an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters are present, and are an explicit NULL.

When encoded, the `AlgorithmIdentifier` for RSA keys is be byte-for-byte identical with the following hex-encoded bytes: `300d06092a864886f70d0101010500`.

7.1.3.2 SIGNATURE ALGORITHMIDENTIFIER

All objects signed by a TunTrust CA Private Key MUST conform to the CA/B Forum Baseline Requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier-derived type in the co-ntext of signatures.

No other encodings are permitted for these fields.

When encoded, the `AlgorithmIdentifier` is byte-for-byte identical with the specified hex-encoded bytes: RSASSA-PKCS1-v1_5 with SHA-256: `300d06092a864886f70d01010b0500`.

TunTrust does not sign SHA-1 hashes over :

- certificates with an EKU extension containing the id-kp-ocspSigning key purpose;
- “TunTrust Services CA” certificates;
- OCSP responses; or
- CRLs.

7.1.4 NAME FORMS

This section details encoding rules that apply to all Certificates issued by a TunTrust CA. Further restrictions may be specified within Section 7.1.2, but these restrictions do not supersede the Baseline requirements.

7.1.4.1 NAME ENCODING

The following requirements apply to all Certificates listed in Section 7.1.2.

For every valid Certification Path (as defined by RFC 5280, Section 6):

- For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate is byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA certificate.
- For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate is byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.

When encoding a Name, TunTrust ensures that:

- Each Name MUST contain an RDNSequence.
- Each RelativeDistinguishedName MUST contain exactly one AttributeTypeAndValue.

- Each RelativeDistinguishedName, if present, is encoded within the RDNSequence in the order that it appears in Section 7.1.4.2.

  – For example, a RelativeDistinguishedName that contains a countryName AttributeTypeAndValue pair MUST be encoded within the RDNSequence before a RelativeDistinguishedName that contains a stateOrProvinceName AttributeTypeAndValue.

- Each Name MUST NOT contain more than one instance of a given AttributeTypeAndValue across all RelativeDistinguishedNames unless explicitly allowed in these Requirements.

Note: Section 7.1.2.2 provides an exception to the above Name encoding requirements when issuing a Cross-Certified Subordinate CA Certificate, as described within that section.

7.1.4.2 SUBJECT ATTRIBUTE ENCODING

The Baseline Requirements document defines requirements for the content and validation of a number of attributes that may appear within the subject field of a tbsCertificate. CAs SHALL NOT include these attributes unless their content has been validated as specified by, and only if permitted by, the relevant certificate profile specified within Section 7.1.2.

CAs that include attributes in the Certificate subject field that are listed in the table below SHALL encode those attributes in the relative order as they appear in the table and follow the specified encoding requirements for the attribute.

Encoding and Order Requirements for Selected Attributes

Attribute	OID	Specification	Encoding Requirements	Max Length [9]
domainComponent	0.9.2342.19200300.100.1.25	RFC 4519	MUST use IA5String	63
countryName	2.5.4.6	RFC 5280	MUST use PrintableString	2
stateOrProvinceName	2.5.4.8	RFC 5280	MUST use UTF8String or PrintableString	128
localityName	2.5.4.7	RFC 5280	MUST use UTF8String or PrintableString	128
postalCode	2.5.4.17	X.520	MUST use UTF8String or PrintableString	40

[9] **Note**: ASN.1 length limits for DirectoryString are expressed as character limits, not byte limits.

streetAddress	2.5.4.9	X.520	MUST use UTF8String or PrintableString	128
organizationName	2.5.4.10	RFC 5280	MUST use UTF8String or PrintableString	64
surname	2.5.4.4	RFC 5280	MUST use UTF8String or PrintableString	64[10]
givenName	2.5.4.42	RFC 5280	MUST use UTF8String or PrintableString	64[11]
organizationalUnitName	2.5.4.11	RFC 5280	MUST use UTF8String or PrintableString	64
commonName	2.5.4.3	RFC 5280	MUST use UTF8String or PrintableString	64

CAs that include attributes in the Certificate subject field that are listed in the table below SHALL follow the specified encoding requirements for the attribute.

Encoding Requirements for Selected Attributes

Attribute	OID	Specification	Encoding Requirements	Max Length [12]
businessCategory	2.5.4.15	X.520	MUST use UTF8String or PrintableString	128
jurisdictionCountry	1.3.6.1.4.1.311.60.2.1.3	Guidelines for the Issuance and	MUST use PrintableString	2

[10] **Note**: Although RFC 5280 specifies the upper bound as 32,768 characters, this was a transcription error from X.520 (08/2005). The effective (interoperable) upper bound is 64 characters.

[11] **Note**: Although RFC 5280 specifies the upper bound as 32,768 characters, this was a transcription error from X.520 (08/2005). The effective (interoperable) upper bound is 64 characters.

[12] **Note**: ASN.1 length limits for DirectoryString are expressed as character limits, not byte limits.

		Management of Extended Validation Certificates		
jurisdictionStateOrProvince	1.3.6.1.4.1.311.60.2.1.2	Guidelines for the Issuance and Management of Extended Validation Certificates	MUST use UTF8String or PrintableString	128
jurisdictionLocality	1.3.6.1.4.1.311.60.2.1.1	Guidelines for the Issuance and Management of Extended Validation Certificates	MUST use UTF8String or PrintableString	128
serialNumber	2.5.4.5	RFC 5280	MUST use PrintableString	64
organizationIdentifier	2.5.4.97	X.520	MUST use UTF8String or PrintableString	None

7.1.4.3 Subscriber Certificate Common Name Attribute

If present, this attribute MUST contain exactly one entry that is one of the values contained in the Certificate's subjectAltName extension (see Section 7.1.4.2). Since the value of the field is Fully-Qualified Domain Name or Wildcard Domain Name, then it MUST be encoded as a character-for-character copy of the dNSName entry value from the subjectAltName extension. Specifically, all Domain Labels of the Fully-Qualified Domain Name or FQDN portion of the Wildcard Domain Name must be encoded as LDH Labels, and P-Labels MUST NOT be converted to their Unicode representation.

7.1.4.4 Other Subject Attributes

When explicitly stated as permitted by the relevant certificate profile specified within Section 7.1.2, CAs MAY include additional attributes within the AttributeTypeAndValue beyond those specified in Section 7.1.4.2.

Before including such an attribute, TunTrust SHALL:

- Document the attributes within Section 7.1.4 of their CP or CPS, along with the applicable validation practices.
- Ensure that the contents contain information that has been verified by the CA, independent of the Applicant.

7.1.5 NAME CONSTRAINTS

The TunTrust Services CA is technically constrained with restrictions to issue SSL Certificate for domain names under the top level domain ".tn" and owned by entities under the Tunisian Jurisdiction.

TunTrust Services CA X509v3 Name Constraints	Permitted: DNS:tn DirName: C = TN Excluded: IP:0.0.0.0/0.0.0.0 IP:0:0:0:0:0:0:0:0/0:0:0:0:0:0:0:0

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

7.1.6.1 RESERVED CERTIFICATE POLICY IDENTIFIERS

7.1.6.2 ROOT CA CERTIFICATES

TunTrust Root CA certificates do not contain any certificatePolicies extension, therefore do not have policy identifiers in them.

7.1.6.3 SUBORDINATE CA CERTIFICATES

TunTrust Issuing CAs contain the following policy identifiers (as described in Appendix A):

- TunTrust Services CA: 2.16.788.1.2.7.1.1.2 ;

7.1.6.4 SUBSCRIBER CERTIFICATES

SSL certificates must contain the certificate policy identifier 2.23.140.1.2.2.

The certificate policy identifiers of the Subscriber Certificates are listed in the certificate policies extension in Appendix B.

TunTrust Issuing CAs assert that the Certificates it issues containing the specified policy identifiers listed in the certificate policies extension in Appendix B, are managed in accordance with the CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates.

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

Since the pathLenConstraint is set to zero, no policy constraints were placed on the Issuing CAs.

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

TunTrust does not include anything in the Policy Qualifier field of the certificatePolicies extension.

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION

The certificate policies extension is set to non-critical in TunTrust CAs and Subscribers certificates.

7.2 CRL PROFILE

Prior to 2024-03-15, TunTrust SHALL issue CRLs in accordance with the profile specified in the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates or the profile specified in its 1.8.7 Version. Effective 2024-03-15, TunTrust SHALL issue CRLs in accordance with the profile specified in the current version of the Baseline Requirements.

All CRLs that TunTrust issues comply with the following CRL profile, which incorporates, and is derived from RFC 5280. Except as explicitly noted, all normative requirements imposed by RFC 5280 shall apply, in addition to the normative requirements imposed by the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. TunTrust CRL profiles description is available in Appendix C of this CP/CPS.

A full and complete CRL is a CRL whose scope includes all Certificates issued by the CA.

A partitioned CRL (sometimes referred to as a “sharded CRL”) is a CRL with a constrained scope, such as all Certificates issued by the CA during a certain period of time (“temporal sharding”). Aside from the presence of the Issuing Distribution Point extension (OID 2.5.29.28) in partitioned CRLs, both CRL formats are syntactically the same from the perspective of this profile.

TunTrust issues a full and complete CRL and does not issue partitioned CRL nor indirect CRLs (i.e., the issuer of the CRL is not the issuer of all Certificates that are included in the scope of the CRL).

Field	Presence	Description
tbsCertList		
version	MUST	MUST be v2(1), see Section 7.2.1
signature	MUST	See Section 7.1.3.2
issuer	MUST	MUST be byte-for-byte identical to the subject field of the Issuing CA.
thisUpdate	MUST	Indicates the issue date of the CRL.
nextUpdate	MUST	Indicates the date by which the next CRL will be issued. For CRLs covering Subscriber Certificates, at most 10 days after the thisUpdate. For other CRLs, at most 12 months after the thisUpdate.
revokedCertificates	*	MUST be present if the CA has issued a Certificate that has been revoked and the corresponding entry has yet to appear on at least one regularly scheduled CRL beyond the

		revoked Certificate's validity period. The CA SHOULD remove an entry for a corresponding Certificate after it has appeared on at least one regularly scheduled CRL beyond the revoked Certificate's validity period. See the "revokedCertificates Component" table for additional requirements.
extensions	MUST	See the "CRL Extensions" table for additional requirements.
signatureAlgorithm	MUST	Encoded value MUST be byte-for-byte identical to the tbsCertList.signature.
signature	MUST	-
Any other value	NOT RECOMMENDED	-

7.2.1 VERSION NUMBER(S)

The TunTrust CAs issue X.509 Version 2 CRLs in accordance with IETF PKIX RFC 5280.

7.2.2 CRL AND CRL ENTRY EXTENSIONS

CRL Extensions

Extension	Presence	Critical	Description
authorityKeyIdentifier	MUST	N	See Section **Erreur ! Source du renvoi introuvable.** 7.1.2.11.1
CRLNumber	MUST	N	MUST contain an INTEGER greater than or equal to zero (0) and less than 2^{159}, and convey a strictly increasing sequence.
IssuingDistributionPoint	*	Y	See Section 7.2.2.1 CRL Issuing Distribution Point
Any other extension	NOT RECOMMENDED	-	-

revokedCertificates Component

Component	Presence	Description
serialNumber	MUST	MUST be byte-for-byte identical to the serialNumber contained in the revoked Certificate.
revocationDate	MUST	Normally, the date and time revocation occurred. See the footnote following this table for circumstances where backdating is permitted.
crlEntryExtensions	*	See the "crlEntryExtensions Component" table for additional requirements.

Note: TunTrust will update the revocation date in a CRL entry when it is determined that the private key of the Certificate was compromised prior to the revocation date that is indicated in the CRL entry for that Certificate. Backdating the revocationDate field is an exception to best practice described in RFC 5280 (Section 5.3.2); however, these requirements

specify the use of the revocationDate field to support TLS implementations that process the revocationDate field as the date when the Certificate is first considered to be compromised.

crlEntryExtensions Component

CRL Entry Extension	Presence	Description
reasonCode	*	When present (OID 2.5.29.21), MUST NOT be marked critical and MUST indicate the most appropriate reason for revocation of the Certificate. MUST be present unless the CRL entry is for a Certificate not technically capable of causing issuance and either 1) the CRL entry is for a Subscriber Certificate subject to these Requirements revoked prior to July 15, 2023 or 2) the reason for revocation (i.e., reasonCode) is unspecified (0). See the "CRLReasons" table for additional requirements.
Any other value	NOT RECOMMENDED	-

CRLReasons

RFC 5280 reasonCode	RFC 5280 reasonCode value	Description
unspecified	0	Represented by the omission of a reasonCode. MUST be omitted if the CRL entry is for a Certificate not technically capable of causing issuance unless the CRL entry is for a Subscriber Certificate subject to these Requirements revoked prior to July 15, 2023.
keyCompromise	1	Indicates that it is known or suspected that the Subscriber's Private Key has been compromised.
affiliationChanged	3	Indicates that the Subject's name or other Subject Identity Information in the Certificate has changed, but there is no cause to suspect that the Certificate's Private Key has been compromised.
superseded	4	Indicates that the Certificate is being replaced because: the Subscriber has requested a new Certificate, the CA has reasonable evidence that the validation of domain authorization or control for any fully-qualified domain name or IP address in the Certificate should not be relied upon, or the CA has revoked the Certificate for compliance reasons such as the Certificate does not comply with these Baseline Requirements or the CA's CP or CPS.
cessationOfOperation	5	Indicates that the website with the Certificate is shut down prior to the expiration of the Certificate, or if the Subscriber no longer owns or controls the Domain Name in the Certificate prior to the expiration of the Certificate.

RFC 5280 reasonCode	RFC 5280 reasonCode value	Description
certificateHold	6	MUST NOT be included if the CRL entry is for 1) a Certificate subject to these Requirements, or 2) a Certificate not subject to these Requirements and was either A) issued on-or-after 2020-09-30 or B) has a notBefore on-or-after 2020-09-30.
privilegeWithdrawn	9	Indicates that there has been a subscriber-side infraction that has not resulted in keyCompromise, such as the Certificate Subscriber provided misleading information in their Certificate Request or has not upheld their material obligations under the Subscriber Agreement or Terms of Use.

The Subscriber Agreement, and any online resource referenced therein, informs Subscribers about the revocation reason options listed above and provides explanation about when to choose each option. The tools that TunTrust provides to the Subscriber allow for these options to be easily specified when the Subscriber requests revocation of their Certificate, with the default value being that no revocation reason is provided (i.e. the default corresponds to the CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL).

The privilegeWithdrawn reasonCode is not made available to the Subscriber as a revocation reason option, because the use of this reasonCode is determined by TunTrust and not the Subscriber.

When TunTrust obtains verifiable evidence of Key Compromise for a Certificate whose CRL entry does not contain a reasonCode extension or has a reasonCode extension with a non-keyCompromise reason, TunTrust will update the CRL entry to enter keyCompromise as the CRLReason in the reasonCode extension when this is technically possible.

7.2.2.1 CRL ISSUING DISTRIBUTION POINT

TunTrust does not issue partitioned CRLS.

TunTrust does not assert both of the onlyContainsUserCerts and onlyContainsCACerts fields.

The indirectCRL and onlyContainsAttributeCerts fields are set to FALSE (i.e., not asserted).

The onlySomeReasons field is not included; as TunTrust issues full and complete CRLs.

7.3 OCSP PROFILE

The TunTrust OCSP functionality is built according to RFC 6960.

The TunTrust provides uninterrupted on-line Certificate status protocol OCSP support which is a real time Certificate status inquiry. By this service, when appropriate Certificate status inquiries are received, the status of Certificates and additional information as required by the protocol are returned to the inquirer as the response.

If an OCSP response is for a Root CA and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus is present.

The CRLReason indicated contains a value permitted for CRLs, as specified in Section 7.2.2.

7.3.1 VERSION NUMBER

The OCSP service provided by TunTrust supports the v1 protocol version under the "IETF RFC 6960 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP" document.

7.3.2 OCSP EXTENSIONS

TunTrust OCSP profile description is available in Appendix D of this CP/CPS.

The singleExtensions of an OCSP response does not contain the reasonCode (OID 2.5.29.21) CRL entry extension.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

TunTrust is a government entity licensed by Tunisian Law to act as a National Certification Authority. TunTrust operates at all times in compliance to the following:

1. the requirements of this CP/CPS;
2. the latest version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates of the CA/B Forum; and
3. the latest versions of the WebTrust Principles and Criteria For Certification Authorities – SSL Baseline With Network Security and the WebTrust Principles And Criteria For Certification Authorities.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

Although TunTrust issuing CA is technically constrained, all TunTrust CAs are subject to full audit as specified in section 8 of this CP/CPS.

An annual audit is performed by an independent external auditor to assess TunTrust's compliance with requirements set forth above.

An audit period must not exceed one year in duration. In addition to that, more than one compliance audit per year is possible if this is requested by TunTrust or is a result of unsatisfactory results of a previous audit.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

TunTrust's audit is performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.1 of the CA/B Forum Baseline Requirements);
3. For audits conducted in accordance with the WebTrust standard licensed by WebTrust;
4. For audits conducted in accordance with any one of the ETSI standards accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403;
5. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function; and

6. Bound by law, government regulation, or professional code of ethics.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

TunTrust utilizes independent auditors that do not have any financial interest or business relationship that could foreseeably create a significant bias for or against TunTrust.

8.4 TOPICS COVERED BY ASSESSMENT

TunTrust undergoes an audit in accordance with the current versions of WebTrust for CAs and WebTrust for CAs SSL Baseline with Network Security. Topics covered in this annual audit include, but are not limited to, the requirements of this CP/CPS, environmental controls, CA key management, and certificate life cycle management.

The chosen audit scheme incorporates periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

The audit is conducted by a Qualified Auditor, as specified in Section 8.2.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

With respect to compliance audits of TunTrust's operations, significant exceptions or deficiencies identified during the compliance audit will result in a determination of actions to be taken. This determination is made by TunTrust Board of Directors with input from the auditor. If exceptions or deficiencies are identified, TunTrust management is responsible for developing and implementing a corrective action plan. Once the plan has been implemented, TunTrust will call for an auxiliary audit to verify that the noted deficiencies have been remediated.

If the deficiency is deemed so serious, or the time to remediate so long as to call into question the integrity of certificates issued, TunTrust CA will inform the relevant browser root certificate program managers that a serious deficiency in practice has been uncovered, and that they should take such steps as to mitigate the risk to their program's integrity.

If the deficiency is deemed so serious, or the time to remediate so long as to call into question the integrity of certificates issued, TunTrust CA will inform the relevant root certificate program managers that a serious deficiency in practice has been uncovered, and that they should take such steps as to mitigate the risk to their program's integrity.

8.6 COMMUNICATION OF RESULTS

TunTrust makes the Audit Report publicly available at https://www.tuntrust.tn/repository. The results will also be sent to any other appropriate entities that may be entitled by law, regulation, or agreement to receive a copy of the audit results. Such parties include the relevant browser root certificate program managers.

TunTrust makes its Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, and if so requested by an Application Software Supplier, TunTrust will provide an explanatory letter signed by the Qualified Auditor.

The Audit Report contains at least the following clearly-labeled information:

1. name of the organization being audited;
2. name and address of the organization performing the audit;
3. the SHA-256 fingerprint of all Roots and Subordinate CA Certificates, including Cross-Certified Subordinate CA Certificates, that were in-scope of the audit;
4. audit criteria, with version number(s), that were used to audit each of the certificates (and associated keys);
5. a list of the CA policy documents, with version numbers, referenced during the audit;
6. whether the audit assessed a period of time or a point in time;
7. the start date and end date of the Audit Period, for those that cover a period of time;
8. the point in time date, for those that are for a point in time;
9. the date the report was issued, which will necessarily be after the end date or point in time date.

An authoritative English language version of the publicly available audit information MUST be provided by the Qualified Auditor and TunTrust will ensure it is publicly available.

The Audit Report MUST be available as a PDF, and SHALL be text searchable for all information required. Each SHA-256 fingerprint within the Audit Report MUST be uppercase letters and MUST NOT contain colons, spaces, or line feeds.

8.7 Self-Audits

TunTrust performs regular internal audits of its operations, personnel, and compliance with this CP/CPS.

During the period in which TunTrust issues Certificates, TunTrust monitors adherence to this CP/CPS and the CA/B Forum Baseline Requirements and strictly control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one Certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

TunTrust uses a Linting process to verify the technical accuracy of Certificates within the selected sample set independently of previous linting performed on the same Certificates.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

TunTrust charges fees for issuing of Certificates according to the respective price list published on their website https://www.tuntrust.tn or made available upon request.

The update of the fees goes through the Board of Directors of TunTrust. After a favorable opinion, TunTrust forwards the proposal to the Ministry of Information Technology of Tunisia for approval.

9.1.2 Certificate access fees

TunTrust does not charge fees for access to its Certificate databases.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES

TunTrust does not charge a Certificate revocation fee or a fee for checking the validity status of an issued Certificate using a CRL or the OCSP.

9.1.4 FEES FOR OTHER SERVICES

TunTrust may elect to charge fees for its other services. Such fees will be outlined in the applicable Subscriber agreement.

9.1.5 REFUND POLICY

TunTrust does not refund the fees of Certificates.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 INSURANCE COVERAGE

TunTrust currently maintains a commercial general liability insurance according to the National Law.

9.2.2 OTHER ASSETS

Since TunTrust is a governmental entity, it shall have access to other resources to support operations and pay damages for potential liability, which may be couched in terms of a minimum level of assets necessary to operate and cover contingencies that might occur within TunTrust PKI.

9.2.3 INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES

No warranty coverage is available for Subscribers and Relying Parties except the warranties listed in section 9.6.1.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 SCOPE OF CONFIDENTIAL INFORMATION

TunTrust keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel. Confidential information includes, but is not limited to:

- Private Keys;
- Activation data used to access Private Keys or to gain access to the CA system;
- Disaster Recovery, and Business Continuity Plans ;
- Any certificate application records and documentation submitted in support of certificate applications, which is not in relation to an issued certificate, whether successful or rejected ;
- External or internal audit trail records and reports, which are not required to be openly published ;
- Transaction records, financial audit records, and internal records on the operations of TunTrust's infrastructure, certificate management, services and data.

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

The following are not considered confidential:

- Certificates;
- Certificate revocation Lists;
- CP/CPS; and
- any information available in TunTrust repository at https://www.tuntrust.tn/repository.

9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

TunTrust protects and secures confidential information from disclosure. All employees of TunTrust are bound by TunTrust Information Security Policy and required by the security chart engagements to preserve the confidentiality of information so labeled.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 PRIVACY PLAN

TunTrust protects personal information in accordance with the Tunisian law N° 2004-63of July 27th, 2004 on the protection of personal data and TunTrust internal document.

TunTrust makes available to Subscribers and Relying Parties the company Privacy Policy on the website https://www.tuntrust.tn/repository.

9.4.2 INFORMATION TREATED AS PRIVATE

TunTrust treats all personal information about an individual that is not publicly available in the contents of a Certificate, CRL or OCSP as private information. TunTrust protects private information using appropriate safeguards and a reasonable degree of care.

9.4.3 INFORMATION NOT DEEMED PRIVATE

Private information does not include Certificates, CRLs, and the personal or corporate information appearing in them.

9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

TunTrust employees and contractors are expected to handle personal information in strict confidence and meet the requirements of Tunisia law concerning the protection of personal data. All sensitive information is securely stored and protected against accidental disclosure.

9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION

Personal information obtained from an Applicant during the application or identity verification process is considered private information if the information is not included in a Certificate. As part of a Subscriber Agreement, all Subscribers consent to the global transfer of any personal data contained in the Certificate and

agree to allow TunTrust to handle any private information required for the issuance and maintenance of certificates.

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

TunTrust will only release or disclose private information on judicial or other authoritative order.

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

TunTrust is not required to release any confidential information, unless as otherwise required by law, without an authenticated, reasonably specific request by a legal entity as stated in section 9.4.6.

9.5 INTELLECTUAL PROPERTY RIGHTS

TunTrust does not knowingly violate the intellectual property rights of third parties. Public and Private Keys remain the property of Subscribers who legitimately hold them.

TunTrust owns the intellectual property rights in TunTrust's services, including the certificates, trademarks used in providing the services, and this CP/CPS. Certificate and revocation information are the property of TunTrust.

TunTrust grants permission to reproduce and distribute Certificates on a non-exclusive, royalty free basis, provided that they are reproduced and distributed in full.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA REPRESENTATIONS AND WARRANTIES

By issuing a Certificate, TunTrust makes the Certificate warranties listed herein to the following Certificate Beneficiaries:

- The Subscriber that is a party to the Subscriber Agreement ;
- All Application Software Suppliers with whom TunTrust has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
- All Relying Parties who reasonably rely on a Valid Certificate.

TunTrust represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, TunTrust has complied with the CA/B Forum Baseline Requirements and this CP/CPS in issuing and managing the Certificate. The Certificate Warranties specifically include, but are not limited to, the following:

1. **Right to Use Domain Nam**e: That, at the time of issuance, TunTrust (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP/CPS;
2. **Authorization for Certificate:** That, at the time of issuance, TunTrust (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP/CPS;

3. **Accuracy of Information:** That, at the time of issuance, TunTrust (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CP/CPS;
4. **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, TunTrust
   (i) implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.2 and 7.1.2;
   (ii) followed the procedure when issuing the Certificate; and
   (iii) accurately described the procedure in this CP/CPS;
5. **Subscriber Agreement:** That, if TunTrust and the Subscriber are not Affiliated, the Subscriber and TunTrust are parties to a legally valid and enforceable Subscriber Agreement that satisfies the CA/B Forum Baseline Requirements, or, if TunTrust and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;
6. **Status:** That TunTrust maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
7. **Revocation:** That TunTrust will revoke the Certificate for any of the reasons specified in the CA/B Forum Baseline Requirements.

9.6.2 RA REPRESENTATIONS AND WARRANTIES

TunTrust RA represents that:

- Information provided by TunTrust RA does not contain any false or misleading information, and
- All Certificates requested by TunTrust RA meet the requirements of the applicable CP/CPS.

9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

TunTrust requires, as part of the Subscriber Agreement, that the Applicant makes the commitments and warranties in this section for the benefit of TunTrust and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, TunTrust obtains, for the express benefit of TunTrust and the Certificate Beneficiaries, the Applicant's agreement to the Subscriber Agreement with TunTrust CA.

TunTrust implements a process to ensure that each Subscriber Agreement is legally enforceable against the Applicant. In either case, the Agreement is applied to the Certificate to be issued pursuant to the Certificate request.

A separate Agreement is used for each Certificate request, or a single Agreement is used to cover multiple future Certificate requests and the resulting Certificates, so long as each Certificate that TunTrust issues to the Applicant is clearly covered by that Subscriber Agreement.

The Subscriber Agreement contains provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. **Accuracy of Information:** An obligation and warranty to provide accurate and complete information at all times to TunTrust, both in the Certificate request and as otherwise requested by TunTrust in connection with the issuance of the Certificate(s) to be supplied by TunTrust;
2. **Protection of Private Key:** An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);

3. **Acceptance of Certificate:** An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
4. **Use of Certificate:** An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement;
5. **Reporting and Revocation:** An obligation and warranty to: (a) promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate ;
6. **Termination of Use of Certificate:** An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise ;
7. **Responsiveness:** An obligation to respond to TunTrust's instructions concerning Key Compromise or Certificate misuse within a specified time period ;
8. **Acknowledgment and Acceptance:** An acknowledgment and acceptance that TunTrust is entitled to revoke the Certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or if revocation is required by the present CP/CPS, or the CA/B Forum Baseline Requirements.

9.6.4 RELYING PARTY REPRESENTATIONS AND WARRANTIES

Each Relying Party represents that, prior to relying on a TunTrust Certificate, it:

- Obtained sufficient knowledge on the use of digital Certificates and PKI,
- Studied the applicable limitations on the usage of Certificates and agrees to TunTrust's limitations on liability related to the use of Certificates,
- Has read, understands, and agrees to this CP/CPS,
- Verified both the TunTrust Certificate and the Certificates in the Certificate chain using the relevant CRL or OCSP,
- Will not use a TunTrust Certificate if the Certificate has expired or been revoked, and
- Will take all reasonable steps to minimize the risk associated with relying on a TunTrust Certificate after considering:
  - applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction,
  - the intended use of the Certificate as listed in the Certificate or this CP/CPS,
  - the data listed in the Certificate,
  - the potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,
  - the Relying Party's previous course of dealing with the Subscriber,
  - the Relying Party's understanding of trade, including experience with computer-based methods of trade, and
  - any other indication of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

Any unauthorized reliance on a Certificate is at a party's own risk.

9.6.5 REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS

No implied or express warranties are given by TunTrust to other participants other than in Subscriber agreements, Relying Party agreements and any other agreements signed by TunTrust with Third Parties.

9.7 DISCLAIMERS OF WARRANTIES

To the extent permitted by applicable law, this CP/CPS, the Subscriber Agreement, the Relying Party Agreement and any other contractual agreement applicable within the TunTrust PKI shall disclaim TunTrust possible warranties, including any warranty of merchantability or fitness for a particular purpose.

To the extent permitted by applicable law, TunTrust makes no express or implied representations or warranties pursuant to this CP/CPS. TunTrust expressly disclaims any and all express or implied warranties of any type to any person, including any implied warranty of title, non-infringement, merchantability, or fitness for a particular purpose.

9.8 LIMITATIONS OF LIABILITY

TunTrust is only liable for damages which are the result of its failure to comply with this CP/CPS and which were provoked deliberately or wantonly negligent.

TunTrust is not in any event liable for any loss of profits, indirect and consequential damages, or loss of data, to the extent permitted by applicable law. TunTrust is not liable for any damages resulting from infringements by the Subscriber or the Relying Party on the applicable terms and conditions.

TunTrust is not in any event liable for damages that result from force major events as detailed in section 9.15. TunTrust takes commercially reasonable measures to mitigate the effects of force major in due time. Any damages resulting of any delay caused by force major will not be covered by TunTrust.

The Subscriber is liable to TunTrust and Relying Parties for any damages resulting from misuse, willful misconduct, failure to meet regulatory obligations, or noncompliance with other provisions for using the Certificate.

9.9 INDEMNITIES

9.9.1 INDEMNIFICATION BY TUNTRUST

Notwithstanding any limitations on its liability to Subscriber and Relying Parties, TunTrust acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with TunTrust do not assume any obligation or potential liability of TunTrust under this CP/CPs or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. TunTrust shall defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by TunTrust, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by TunTrust where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from

TunTrust online, and the application software either failed to check such status or ignored an indication of revoked status).

Additional indemnity provisions and obligations are contained within relevant contractual agreements such as the Subscriber Agreement and Relying Party Agreement.

9.9.2 INDEMNIFICATION BY SUBSCRIBERS

To the extent permitted by law, each Subscriber shall release, indemnify and hold harmless TunTrust CA, and all TunTrust directors, shareholders, officers, agents, employees, contractors and successors of the foregoing, against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of its Subscriber Agreement, this CP/CPS, or applicable law; (iii) the compromise or unauthorized use of a certificate or Private Key caused by the Subscriber's negligence or intentional acts; or (iv) Subscriber's misuse of a certificate or Private Key.

9.9.3 INDEMNIFICATION BY RELYING PARTIES

To the extent permitted by law, each Relying Party shall release, indemnify and hold harmless TunTrust CA, and all TunTrust directors, shareholders, officers, agents, employees, contractors and successors of the foregoing against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of any service terms applicable to the services provided by TunTrust or its affiliates and used by the Relying Party, this CP/CPS, or applicable law; (ii) unreasonable reliance on a certificate; or (iii) failure to check the certificate's status prior to use.

9.10 TERM AND TERMINATION

9.10.1 TERM

This CP/CPS and any amendments thereto, are effective upon publication in TunTrust's Repository.

9.10.2 TERMINATION

This CP/CPS, as may be amended from time to time, is effective until replaced by a new version, which shall be published in TunTrust's Repository.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

Upon Termination of this CP/CPS, Subscribers, and Relying Parties are bound by its terms for all Certificates issued, while it's effective, for the remainder of the validity periods of such Certificates.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

TunTrust, Subscribers, Applicants, Relying Parties and other participants will use official means of communication in public service as per Tunisia National Law.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

This CP/CPS is reviewed at least annually and may be reviewed more frequently. Revisions of this CP/CPS are reviewed and approved within TunTrust Board of Directors. Amendments are made by posting an updated version of the CP/CPS to the online repository. Changes to this CP/CPS are indicated by an incremental version number.

9.12.2 NOTIFICATION MECHANISM AND PERIOD

Updates, amendments, and new versions of TunTrust's CP/CPS shall be posted in TunTrust's repository. Such publication shall serve as notice to all relevant entities.

9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

If TunTrust's Board of Directors determines that a change is necessary in the object identifier corresponding to this CP/CPS, the amendment shall contain new object identifiers for this CP/CPS. Otherwise, amendments shall not require a change in Certificate policy object identifier.

9.13 DISPUTE RESOLUTION PROVISIONS

Parties are required to notify TunTrust and attempt to resolve disputes directly with TunTrust before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution.

9.14 GOVERNING LAW

This CP/CPS is governed, construed and interpreted in accordance with the laws of Tunisia. This choice of law is made to ensure consistency with TunTrust CA restriction to issue SSL Certificate for entities under the Tunisian jurisdiction. The law of Tunisia applies also to all TunTrust commercial or contractual relationships in which this CP/CPS may apply or quoted implicitly or explicitly in relation to TunTrust products and services where TunTrust acts as a provider, supplier, beneficiary receiver or otherwise.

Each party, including TunTrust partners, Subscribers and Relying Parties, irrevocably submit to the jurisdiction of the district courts of Ariana in Tunisia.

9.15 COMPLIANCE WITH APPLICABLE LAW

TunTrust issues Certificates and operate its PKI in accordance with Tunisian law.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 ENTIRE AGREEMENT

This CP/CPS and the applicable Subscriber Agreement and Relying Party Agreement represent the entire agreement between any Subscriber or Relying Party and TunTrust and shall supersede any and all prior

understandings and representations pertaining to its subject matter. In the event, however, of a conflict between this CP/CPS and any other express agreement between a Subscriber or Relying Party with TunTrust with respect to a Certificate, including but not limited to a Subscriber Agreement or the Relying Party Agreement shall take precedence.

9.16.2 ASSIGNMENT

Entities operating under this CP/CPS cannot assign their rights or obligations without the prior written consent of TunTrust.

9.16.3 SEVERABILITY

In the event of a conflict between the CA/B Forum Baseline Requirements and a Tunisian law, regulation or government order, TunTrust may modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in Tunisia.

This applies only to operations or certificate issuances that are subject to that Law. In such event, TunTrust will immediately (and prior to issuing a certificate under the modified requirement) include in this section a detailed reference to the Law requiring a modification of the CA/B Forum Baseline Requirements under this section, and the specific modification to the Baseline Requirements implemented by TunTrust.

TunTrust will also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CP/CPS.

Any modification to TunTrust practice enabled under this section will be discontinued if and when the Law no longer applies, or the Baseline Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to this CP/CPS and a notice to the CA/Browser Forum, as outlined above, is made within 90 days.

9.16.4 ENFORCEMENT (ATTORNEYS' FEES AND WAIVER OF RIGHTS)

TunTrust may seek indemnification and any fees (including reasonable attorney's fees and court costs) from a party for damages, losses and expenses related to that party's conduct.

TunTrust's failure to enforce a provision of this CP/CPS does not waive TunTrust's right to enforce the same provision later, or right to enforce any other provision of this CP/CP.

9.16.5 FORCE MAJEURE

TunTrust is not liable for any delay or failure to perform an obligation under this CP/CPS to the extent that the delay or failure is caused by an occurrence beyond TunTrust's reasonable control. The operation of the Internet is beyond TunTrust's reasonable control.

9.17 OTHER PROVISIONS

The present CP/CPS does not state any conditions in this respect.

APPENDIX A: TUNTRUST CA CERTIFICATE PROFILES

1. TunTrust Root CA

The following table describes the certificate profile of TunTrust Root CA:

Fields	Critical	Values
Version		3 (0x2)
Serial Number		13:02:d5:e2:40:4c:92:46:86:16:67:5d:b4:bb:bb:b2:6b:3e:fc:13
Signature Algorithm		sha256WithRSAEncryption
Issuer		C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Root CA
Validity		
Not Before		Apr 26 08:57:56 2019 GMT
Not After		Apr 26 08:57:56 2044 GMT
Subject		C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Root CA
Subject Public Key Info		
Public Key Algorithm		rsaEncryption
RSA Public Key		4096 bits
Exponent		65537 (0x10001)
X509v3 extensions		
X509v3 Subject Key Identifier		SHA-1 Hash of Subject public key
X509v3 Basic Constraints	True	CA: TRUE
X509v3 Authority Key Identifier		Keyid: 06:9A:9B:1F:53:7D:F1:F5:A4:C8:D3:86:3E:A1:73:59:B4:F7:44:21
X509v3 Key Usage	True	Certificate Sign, CRL Sign
Signature Algorithm		sha256WithRSAEncryption

2. TunTrust Services CA

The following table describes the certificate profile of TunTrust Services CA:

Fields	Critical	Values
Version		3 (0x2)
Serial Number		60:1a:7c:2f:60:93:b7:a6:73:da:5f:8c:9c:88:5f:37:a7:58:97:c0
Signature Algorithm		sha256WithRSAEncryption
Issuer		C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Root CA
Validity		
Not Before		Apr 26 10:23:31 2019 GMT
Not After		Apr 26 10:23:31 2039 GMT
Subject		C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Services CA
Subject Public Key Info		
Public Key Algorithm		rsaEncryption
RSA Public Key		4096 bits
Exponent		65537 (0x10001)
X509v3 extensions		
X509v3 Name Constraints	True	Permitted: DNS:tn DirName: C = TN Excluded: IP:0.0.0.0/0.0.0.0 IP:0:0:0:0:0:0:0:0/0:0:0:0:0:0:0:0
Authority Information Access		CAIssuers - URI:http://www.tuntrust.tn/pub/TnTrustRootCA.crt OCSP - URI:http://va.tuntrust.tn
X509v3 Subject Key Identifier		9F:25:17:CE:6F:90:AB:61:2F:C1:47:A9:E0:2F:99:13:5D:FA:23:39
X509v3 Basic Constraints	True	CA: TRUE, pathlen:0
X509v3 Authority Key Identifier		Keyid: 06:9A:9B:1F:53:7D:F1:F5:A4:C8:D3:86:3E:A1:73:59:B4:F7:44:21
X509v3 Certificate Policies		Policy: 2.16.788.1.2.7.1.1.2
X509 CRL Distribution Points		URI:http://crl.tuntrust.tn/tntrustrootca.crl
X509v3 Key Usage	True	Certificate Sign, CRL Sign
X509v3 Extended Key Usage		TLS Web Server Authentication, TLS Web Client Authentication

Signature Algorithm		sha256WithRSAEncryption

APPENDIX B : TUNTRUST PKI END-ENTITY PROFILES

1. OVCP SSL 186 days

The following table provides the description of the fields for TunTrust OVCP SSL 186 days Certificate issued under TunTrust Services CA.

Base Profile	Included	Critical	O/M [13]	CO [14]	Values
Data:					
Version	X	False	M	S	3 (0x2)
Serial Number	X	False	M	FDV	Validated on duplicates
Signature Algorithm	X	False	M	S	SHA256 with RSA Encryption
Issuer	X	False	M	S	C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Services CA
Validity					
Not Before	X	False	M	D	Certificate generation process date/time
Not After	X	False	M	D	Certificate generation process date/time + 186 days.
Subject					
C, countryName	X	False	M	S	TN
L, localityName	X	False	M	D	Location in which the company's registered office is established.
O, OrganizationName	X	False	M	D	Contains the full registered name of the organization as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA.
serialNumber	X	False	M	D	The SerialNumber attribute guarantees the uniqueness of the DN in the Certificate and is constructed by TunTrust RA.

13. O/M: O = Optional, M = Mandatory.

14. CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

CN, commonName	X	False	M	D	This field contains exactly one entry that is one of the values contained in the Certificate's 'subjectAltName' extension (see Section 7.1.4.2.1 of the Baseline Requirements). Since the value of this field is a Fully-Qualified Domain Name or Wildcard Domain Name, then this value MUST be encoded as a character-for-character copy of the `dNSName` entry value from the `subjectAltName` extension. Specifically, all Domain Labels of the Fully-Qualified Domain Name or FQDN portion of the Wildcard Domain Name must be encoded as LDH Labels, and P-Labels MUST NOT be converted to their Unicode representation.
Subject Public Key Info:					
Public Key Algorithm	X	False	M	S	rsaEncryption
RSA Public Key	X	False	M	S	(2048 bit)
Modulus (2048 bit)	X	False	M	S	
Exponent	X	False	M	S	65537 (0x10001)
X509v3 extensions					
Authority Information Access	X	False	M	S	CA Issuers - URI:http://www.tuntrust.tn/pub/TunTrustServicesCA.crt OCSP - URI:http://va.tuntrust.tn
X509v3 Subject Key Identifier:	X	False	M	D	This extension identifies the public key being certified.
X509v3 Basic Constraints:	X	True	M	S	CA:False
X509v3 Authority Key Identifier	X	False	M	S	keyid:9F:25:17:CE:6F:90:AB:61:2F:C1:47:A9:E0:2F:99:13:5D:FA:23:39
X509v3 Certificate Policies	X	False	M	S	Policy: 2.23.140.1.2.2 Policy: 2.16.788.1.2.7.1.1.2.1 Policy : 0.4.0.2042.1.7
X509v3 CRL Distribution Points	X	False	M	S	URI:http://crl.tuntrust.tn/tuntrustservicesca.crl
X509v3 Key Usage	X	True	M	S	Digital Signature, Key Encipherment
X509v3 Extended Key Usage	X	False	M	S	TLS Web Server Authentication

X509v3 Subject alternative Name	X	False	M	D	DNS: FQDN (Fully-Qualified Domain Name) of application/server.

2. OVCP SSL 30 days

The following table provides the description of the fields for TunTrust OVCP SSL 30 days Certificate issued under TunTrust Services CA.

Base Profile	Included	Critical	O/M[15]	CO[16]	Values
Data:					
Version	X	False	M	S	3 (0x2)
Serial Number	X	False	M	FDV	Validated on duplicates
Signature Algorithm	X	False	M	S	SHA256 with RSA Encryption
Issuer	X	False	M	S	C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Services CA
Validity					
Not Before	X	False	M	D	Certificate generation process date/time
Not After	X	False	M	D	-Certificate generation process date/time + 30 days.
Subject					
C, countryName	X	False	M	S	TN
L, localityName	X	False	M	S	ARIANA
O, OrganizationName	X	False	M	S	AGENCE NATIONALE DE CERTIFICATION ELECTRONIQUE

15. O/M: O = Optional, M = Mandatory.

16. CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

serialNumber	X	False	M	D	The SerialNumber attribute guarantees the uniqueness of the DN in the Certificate and is constructed by TunTrust.
CN, commonName	X	False	M	S	validovssl.tuntrust.tn
Subject Public Key Info:					
Public Key Algorithm	X	False	M	S	rsaEncryption
RSA Public Key	X	False	M	S	(2048 bit)
Modulus (2048 bit)	X	False	M	S	
Exponent	X	False	M	S	65537 (0x10001)
X509v3 extensions					
Authority Information Access	X	False	M	S	CA Issuers - URI:http://www.tuntrust.tn/pub/TunTrustServicesCA.crt OCSP - URI:http://va.tuntrust.tn
X509v3 Subject Key Identifier:	X	False	M	D	This extension identifies the public key being certified.
X509v3 Basic Constraints:	X	True	M	S	CA:False
X509v3 Authority Key Identifier	X	False	M	S	keyid:9F:25:17:CE:6F:90:AB:61:2F:C1:47:A9:E0:2F:99:13:5D:FA:23:39
X509v3 Certificate Policies	X	False	M	S	Policy: 2.23.140.1.2.2 Policy: 2.16.788.1.2.7.1.1.2.1 Policy : 0.4.0.2042.1.7
X509v3 CRL Distribution Points	X	False	M	S	URI:http://crl.tuntrust.tn/tuntrustservicesca.crl
X509v3 Key Usage	X	True	M	S	Digital Signature, Key Encipherment
X509v3 Extended Key Usage	X	False	M	S	TLS Web Server Authentication
X509v3 Subject alternative Name	X	False	M	S	validovssl.tuntrust.tn

APPENDIX C : PROFILES OF THE CRL OF TUNTRUST CAS

1. TunTrust Root CA CRL

The following table describes the CRL profile of TunTrust Root CA:

Field	Value
Version	2 (0x1)
Signature Algorithm	sha256WithRSAEncryption
Issuer	/CN=TunTrust Root CA/O=Agence Nationale de Certification Electronique/C=TN
Last Update	CRL generation process date/time.
Next Update	CRL generation process date/time + 365 days
CRL extensions	
X509v3 Authority Key Identifier	6:9A:9B:1F:53:7D:F1:F5:A4:C8:D3:86:3E:A1:73:59:B4:F7:44:21
X509v3 CRL Number	A monotonically increasing sequence number
Revoked Certificates:	
Serial Number	Serial number of the revoked certificate
Revocation Date	Date and time of the revocation
CRL entry extensions:	
X509v3 CRL Reason Code	Code of Reason of revocation
Signature Algorithm	sha256WithRSAEncryption

2. TunTrust Services CA CRL

The following table describes the CRL profile of TunTrust Services CA:

Field	Value
Version	2 (0x1)
Signature Algorithm	sha256WithRSAEncryption
Issuer	/CN=TunTrust Services CA/O=Agence Nationale de Certification Electronique/C=TN
Last Update	CRL generation process date/time.
Next Update	CRL generation process date/time + 6 days
CRL extensions	
X509v3 Authority Key Identifier	9F:25:17:CE:6F:90:AB:61:2F:C1:47:A9:E0:2F:99:13:5D:FA:23:39
X509v3 CRL Number	A monotonically increasing sequence number
Revoked Certificates:	
Serial Number	Serial number of the revoked certificate
Revocation Date	Date and time of the revocation
CRL entry extensions:	
X509v3 CRL Reason Code	Code of Reason of revocation
Signature Algorithm	sha256WithRSAEncryption

APPENDIX D : OCSP PROFILE DESCRIPTION

Base Profile	Included	Critical	O/M[17]	CO[18]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Signature Value	X	False		D	Issuing CA Signature
Issuer DN	X			S	Issuing CA DN
Subject DN	X	False			
commonName	X		M	D	Name of the validation Authority
countryName	X		M	D	Country in which the organization's registered office is established (ISO3166).
OrganizationName	X		M	D	Contains the full registered name of the organization as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA.
Locality	X		M	D	Locality Name
Validity	X	False			
Not Before	X			D	Certificate generation process date/time
Not After	X			D	Certificate generation process date/time + 730 days
subjectPublicKeyInfo	X	False			
Algorithm	X				Public Key: Key length: 2048 bits (RSA)

17. O/M: O = Optional, M = Mandatory.

18. CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

SubjectPublicKey	X		M		Exponent: 65537 (0x10001)
X509v3 extensions					
X509v3 Authority Key Identifier	X				Authority Key Identifier
authorityInfoAccess	X	False			
Authority Information Access	X				OCSP - URI:http://va.certification.tn
X509v3 CRL Distribution Points	X	False		S	URI:URI of the CRL
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
X509v3 Basic Constraints	X	True			CA : FALSE
KeyUsage	X	True			
digitalSignature	X			S	True
certificatePolicies	X	False			
PolicyIdentifier	X				Policy: 0.4.0.2042.1.2 Policy: 2.16.788.1.2.7.1.1.2.2
OCSP No Check	X			S	
Extended Key Usage	X	False			
OCSP Signing	X			S	True